Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Pacific Networks Corp. and	)	GN Docket No. 20-111;
ComNet (USA) LLC	)	ITC-214-20090105-00006;
	)	ITC-214-20090424-00199
	)	

ORDER ON REVOCATION AND TERMINATION

Adopted: March 16, 2022 **Released: March 23, 2022**

By the Commission: Chairwoman Rosenworcel and Commissioners Carr and Starks issuing separate statements.

TABLE OF CONTENTS

I. INTRODUCTION

1. In this Order on Revocation and Termination (Order), we revoke the domestic authority of Pacific Networks Corp. (Pacific Networks) and its wholly-owned subsidiary, ComNet (USA) LLC (ComNet) (collectively, the "Companies"), and revoke and terminate their international authority, pursuant to section 214 of the Communications Act of 1934, as amended (Act).[1] Based on our public

[1] 47 U.S.C. § 214; *Pacific Networks Corp. and ComNet (USA) LLC*, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199, Order to Show Cause, 35 FCC Rcd 3733 (IB, WCB, EB 2020) (*Order to Show Cause*); *Pacific Networks Corp. and ComNet (USA) LLC*, GN Docket No. 20-111, File Nos. ITC-214-
(continued….)

interest analysis under section 214 of the Act and the totality of the record, we find that the present and future public interest, convenience, and necessity is no longer served by the Companies' retention of their section 214 authority.

2. *First*, we find that the Companies are U.S. subsidiaries of a Chinese state-owned entity, and therefore they are subject to exploitation, influence, and control by the Chinese government and are highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight. *Second*, given the changed national security environment with respect to China since the Commission authorized the Companies to provide telecommunications services in the United States, we find that the Companies' ownership and control by the Chinese government raise significant national security and law enforcement risks by providing opportunities for the Companies, their parent entities and affiliates, and the Chinese government to access, monitor, store, and in some cases disrupt and/or misroute U.S. communications, which in turn allow them to engage in espionage and other harmful activities against the United States. *Third*, independent of these concerns, the Companies' conduct and representations to the Commission and Congress demonstrate a lack of trustworthiness and reliability that erodes the baseline level of trust that the Commission and other U.S. government agencies require of telecommunications carriers given the critical nature of the provision of telecommunications service in the United States. *Fourth*, given the record evidence, we find that further mitigation would not address these significant national security and law enforcement concerns. We therefore revoke the Companies' domestic and international section 214 authority. *Fifth*, separate and apart from revocation, we find that the Companies violated the 2009 Letter of Assurances with the Executive Branch agencies,[2] compliance with which is an express condition of the Companies' international section 214 authorizations.[3] We therefore terminate the Companies' international section 214 authorizations. *Sixth*, given the record evidence of significant national security and law enforcement risks concerning the Companies' section 214 authority, we will reclaim the two International Signaling Point Codes (ISPCs) that were provisionally assigned to ComNet in 2001 and in

(Continued from previous page)
20090105-00006, ITC-214-20090424-00199, Order Instituting Proceeding on Revocation and Termination, 36 FCC Rcd 6368 (2021) (*Institution Order*).

[2] Department of Homeland Security, Department of Justice, Petition to Adopt Conditions to Authorizations and Licenses, File Nos. ITC-T/C-20080913-00428, ITC-214-20090105-00006 (filed Mar. 30, 2009); Letter from Norman Yuen, Chairman, Pacific Networks Corp., and Fan Wei, Director, CM Tel (USA) LLC, to Stephen Heifetz, Deputy Assistant Secretary for Policy Development, U.S. Department of Homeland Security, and Matthew G. Olsen, Acting Assistant Attorney General, National Security Division, U.S. Department of Justice (Mar. 3, 2009) (on file in ITC-214-20090105-00006; ITC-T/C-20080913-00428; ITC-214-20090424-00199) (2009 LOA).

[3] Under section 214(c) of the Act, the Commission "may attach to the issuance of the certificate such terms and conditions as in its judgment the public convenience and necessity may require." 47 U.S.C. § 214(c). Pacific Networks' and ComNet's international section 214 authorizations are conditioned upon Pacific Networks and CM Tel (USA) LLC—whose name was changed to ComNet in 2010—abiding by the commitments and undertakings set forth in their 2009 LOA. *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-214-20090105-00006, Public Notice, 24 FCC Rcd 4155, 4156 (IB 2009) (April 9, 2009 Grant Public Notice); *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-214-20090105-00006, Public Notice, 24 FCC Rcd 6379, 6384 (IB 2009) (Corrections) (April 23, 2009 Grant Public Notice); *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-T/C-20080913-00428, Public Notice, 24 FCC Rcd 5376, 5379 (IB 2009) (May 7, 2009 Grant Public Notice); *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-214-19990927-00607, Public Notice, 24 FCC Rcd 5779, 5784 (IB 2009) (May 21, 2009 Grant Public Notice); *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-214-20090424-00199, Public Notice, 25 FCC Rcd 2838, 2841-42 (IB 2010) (Mar. 25, 2010 Informative Public Notice) ("By letter dated February 22, 2010, Applicant notified the Commission that CM Tel (USA) LLC, has changed its name to ComNet (USA) LLC."); Letter from Joshua T. Guyan, Squire, Sanders & Dempsey L.L.P., to International Bureau, FCC (Feb. 22, 2010) (on file in ITC-214-20090424-00199) (Feb. 22, 2010 ComNet Letter).

2003, sixty (60) days from the release date of this Order. *Finally*, we direct the Companies to discontinue any domestic or international services that they provide pursuant to their section 214 authority no later than sixty (60) days from the release of this Order.

II. BACKGROUND

3. A complete procedural history leading to the Commission's adoption of the *Institution Order* on March 17, 2021 is discussed in detail therein.[4] As the Commission stated in the *Institution Order*, Congress created the Commission, among other reasons, "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications . . . ."[5] Promotion of national security is an integral part of the Commission's public interest responsibility, including its administration of section 214 of the Act, and indeed one of the core purposes for which Congress created the Commission.[6] The Commission has taken a number of targeted steps to protect the nation's communications infrastructure from potential security threats,[7] and we continue to do so here.

4. Section 214(a) of the Act prohibits any carrier from constructing, extending, acquiring, or operating any line, and from engaging in transmission through any such line, without first obtaining a certificate from the Commission "that the *present or future* public convenience and necessity require or will require the construction, or operation, or construction and operation, of such additional or extended line . . . ."[8] In 1999, the Commission granted all telecommunications carriers blanket authority under

[4] *See Institution Order*, 36 FCC Rcd at 6374-77, paras. 8-12.

[5] 47 U.S.C. § 151; *Institution Order*, 36 FCC Rcd at 6369, para. 2 (quoting 47 U.S.C. § 151); *see China Telecom (Americas) Corporation*, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Order on Revocation and Termination, FCC 21-114, 2021 WL 5161884 (rel. Nov. 2, 2021) (*China Telecom Americas Order on Revocation and Termination*); *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427, Order on Revocation, FCC 22-9 (rel. Feb. 2, 2022) (*China Unicom Americas Order on Revocation*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs et al.*, WC Docket No. 18-89 et al., Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423 (2019) (*Protecting Against National Security Threats Order*), *aff'd*., *Huawei Technologies USA, Inc. v. FCC*, 2 F.4th 421, 439 (5th Cir. 2021).

[6] 47 U.S.C. § 151; *see Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*; *Market Entry and Regulation of Foreign-Affiliated Entities*, IB Docket Nos. 97-142 and 95-22, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23918-21, paras. 59-66 (1997) (*Foreign Participation Order*), *recon. denied*, *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*, IB Docket 97-142, Order on Reconsideration, 15 FCC Rcd 18158 (2000) (*Reconsideration Order*); *see Protecting Against National Security Threats Order*, 34 FCC Rcd at 11436, para. 34, *aff'd. Huawei Technologies USA v. FCC,* 2 F.4th at 439.

[7] *See, e.g.*, *China Mobile International (USA) Inc.*; *Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, Memorandum Opinion and Order, 34 FCC Rcd 3361, 3365-66, 3376-77, 3380, paras. 8, 31-32, 38 (2019) (*China Mobile USA Order*); *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11433, paras. 26-27; *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7822, paras. 2-3 (2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284, 14285, para. 1 (2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Report and Order, 36 FCC Rcd 11958 (2021); *Institution Order*, 36 FCC Rcd at 6369-70, para. 2; *China Telecom Americas Order on Revocation and Termination* at *2, para. 3; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 3.

[8] 47 U.S.C. § 214(a) (emphasis added); *see Reform of Rules and Policies on Foreign Carrier Entry Into the U.S. Telecommunications Market*, IB Docket No. 12-299, Report and Order, 29 FCC Rcd 4256, para. 2, n.2 (2014) (*ECO Test Report and Order*) ("Any party seeking to provide common carrier telecommunications services between the

(continued….)

section 214 of the Act to provide domestic interstate services and to construct or operate any domestic transmission line.[9] In doing so, the Commission found that the "present and future public convenience and necessity require the construction and operation of all domestic new lines pursuant to blanket authority," subject to the Commission's ability to revoke a carrier's section 214 authority when warranted to protect the public interest.[10] The Commission similarly considers the public interest to determine whether revocation of an international section 214 authorization is warranted. For example, in the *Foreign Participation Order* and the *Reconsideration Order*, the Commission delineated a non-exhaustive list of circumstances where it reserved the right to designate for revocation an international section 214 authorization based on public interest considerations.[11] The Commission initiated revocation proceedings concerning section 214 authorizations in a variety of contexts.[12]

(Continued from previous page)
United States, its territories or possessions, and a foreign point must request authority by application pursuant to section 214(a) of the Act, 47 U.S.C. § 214(a), and section 63.18 of the Commission's rules, 47 C.F.R. § 63.18."). The Supreme Court has determined that the Commission has considerable discretion in deciding how to make its section 214 public interest findings. *FCC v. RCA Communications, Inc.*, 346 U.S. 86, 90 (1953); *see Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Therefor*, CC Docket No. 79-252, First Report and Order, 85 FCC 2d 1, 40-44, paras. 117-29 (1980) (discussing the Commission's authority under section 214(a) of the Act); *Streamlining the International Section 214 Authorization Process and Tariff Requirements*, IB Docket No. 95-118, Notice of Proposed Rulemaking, 10 FCC Rcd 13477, 13480, para. 6 (1995); *Streamlining the International Section 214 Authorization Process and Tariff Requirements*, IB Docket No. 95-118, Report and Order, 11 FCC Rcd 12884, 12903, para. 44 n.63 (1996) (*Streamlining Order*).

[9] *Implementation of Section 402(b)(2)(A) of the Telecommunications Act of 1996*; *Petition for Forbearance of the Independent Telephone & Telecommunications Alliance*, Report and Order and Second Memorandum Opinion and Order, 14 FCC Rcd 11364, 11365-66, para. 2 (1999) (*Domestic 214 Blanket Authority Order*). The Commission did not extend this blanket authority to international services. *Id.* at 11365-66, para. 2 & n.8; 47 CFR § 63.01.

[10] *Domestic 214 Blanket Authority Order*, 14 FCC Rcd at 11374, para. 16. The Commission has explained that it grants blanket section 214 authority, rather than forbearing from application or enforcement of section 214 entirely, in order to remove barriers to entry without relinquishing its ability to protect consumers and the public interest by withdrawing such grants on an individual basis. *Id.* at 11372-73, 11374, paras. 12-14, 16.

[11] *See, e.g.*, *Foreign Participation Order*, 12 FCC Rcd at 24023, para. 295 (where the Commission finds that a U.S. carrier has engaged in anticompetitive conduct); *Reconsideration Order*, 15 FCC Rcd at 18173, para. 28 (where the Commission finds that a U.S. carrier has acquired an affiliation with a foreign World Trade Organization (WTO) carrier and such affiliation poses a very high risk to competition that cannot be remedied by safeguards); *id*., 15 FCC Rcd at 18175-76, para. 35 (where the Commission finds that a U.S. carrier has proposed to acquire a controlling interest in a foreign non-WTO carrier that does not satisfy the effective competitive opportunities (ECO) test or the affiliation may otherwise harm the public interest pursuant to the Commission's policies and rules); *see also* 47 CFR § 63.11(g)(2); *ECO Test Report and Order*, 29 FCC Rcd at 4259, 4266, paras. 6, 22 (eliminating the ECO test which, among other things, had applied to international section 214 applications filed by foreign carriers or their affiliates that have market power in non-WTO Member countries they seek to serve and to notifications filed by authorized U.S. carriers affiliated with or seeking to become affiliated with a foreign carrier that has market power in a non-WTO Member country that the U.S. carrier is authorized to serve, while continuing to reserve the right to proceed to an authorization revocation hearing if the Commission finds that the affiliation may harm the public interest).

[12] *See, e.g.*, *Institution Order*; *China Telecom (Americas) Corporation*, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Order Instituting Proceedings on Revocation and Termination and Memorandum Opinion and Order, 35 FCC Rcd 15006 (2020) (*China Telecom Americas Institution Order*); *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427, Order Instituting Proceeding on Revocation, 36 FCC Rcd 6319 (2021) (*China Unicom Americas Institution Order*); *CCN, Inc. et al.,* Order to Show Cause and Notice of Opportunity for Hearing, 12 FCC Rcd 8547 (1997) (*CCN, Inc. Order to Show Cause*); *CCN, Inc. et al.,* Order, 13 FCC Rcd 13599 (1998) (*CCN, Inc. Order*) (revoking a company's operating authority under section 214 for repeatedly slamming consumers); *Rates for Interstate Inmate Calling Services,* Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 14107, 14170, para. 118 (2013); *Lifeline and Link Up Reform and*
(continued….)

5. As part of the Commission's public interest analysis, the Commission considers a number of factors and examines the totality of the circumstances in each particular situation. One of the factors considered is whether the application for or retention of the authorization raises any national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's or authorization holder's reportable foreign ownership.[13] With regard to this factor, the Commission has sought the expertise of the relevant Executive Branch agencies[14] for 25 years, and has accorded deference to their expertise in identifying such a concern.[15] The Commission has formalized the review process for the Executive Branch agencies to complete their review consistent with Executive Order No. 13913 of April 4, 2020 that established the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee).[16] The Commission ultimately makes an independent

(Continued from previous page)
Modernization et al., Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6785, para. 299 (2012); *Kurtis J. Kintzel et al.*; *Resellers of Telecommunications Services,* Order to Show Cause and Notice of Opportunity for Hearing, 22 FCC Rcd 17197, 17197, 17204-05, 17205-07, paras. 1, 22, 24 (2007) (*Kintzel Order*); *Compass, Inc.*; *Apparent Liability for Forfeiture,* Notice of Apparent Liability for Forfeiture and Order, 21 FCC Rcd 15132, 15141-42, para. 29 (2006); *OneLink Communications, Inc., et al.*, Order to Show Cause, 32 FCC Rcd 1884 (EB-TCD & WCB-CPD 2017).

[13] *See Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66; *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, Report and Order, 35 FCC Rcd 10927, 10963-64, para. 92 (2020) (*Executive Branch Process Reform Report and Order*).

[14] For purposes of this Order, we refer to the following agencies collectively as "Executive Branch agencies": Department of Justice (DOJ), Department of Homeland Security (DHS), Department of Defense (DOD), Department of Commerce, Department of the Treasury, Department of State, Office of Management and Budget, Office of the U.S. Trade Representative, General Services Administration, and Council of Economic Advisers. This list represents a different subset of U.S. government agencies than those that are members of or advisors to the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee). *See* Executive Order No. 13913 of April 4, 2020, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643 (Apr. 8, 2020) (Executive Order 13913); *see also* Letter from Kathy Smith, Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau at 1 (Nov. 16, 2020) (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199) (Executive Branch Nov. 16, 2020 Letter). DOJ, DHS, and DOD also are known informally as "Team Telecom."

[15] *Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66. In the 1997 *Foreign Participation Order*, the Commission affirmed its previously *ad hoc* policy of seeking Executive Branch input on any national security, law enforcement, foreign policy, or trade policy concerns related to the reportable foreign ownership as part of its overall public interest review of an application. In addition to international section 214 authority, the policy also applies to other types of applications with reportable foreign ownership, including applications related to submarine cable landing licenses, assignments or transfers of control of domestic or international section 214 authority, and petitions for declaratory rulings to exceed the foreign ownership benchmarks of section 310(b) of the Act. *Id*.; *Amendment of the Commission's Regulatory Policies to Allow Non-U.S. Licensed Space Stations to Provide Domestic and International Satellite Service in the United States et al.*, IB Docket No. 96-111 et al., Report and Order, 12 FCC Rcd 24094, 24171, paras. 179-80 (1997); *see also Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10928-30, paras. 3-7.

[16] *See generally Executive Branch Process Reform Report and Order*; Executive Order No. 13913, 85 Fed. Reg. at 19643 (stating that, "[t]he security, integrity, and availability of United States telecommunications networks are vital to United States national security and law enforcement interests"); *id*. at 19643-44 (establishing the "Committee," composed of the Secretary of Defense (DOD), the Secretary of Homeland Security (DHS), and the Attorney General of the Department of Justice (DOJ), who serves as the Chair, and the head of any other executive department or agency, or any Assistant to the President, as the President determines appropriate (Members), and also providing for Advisors, including the Secretary of State, the Secretary of Commerce, and the United States Trade Representative (USTR)).

decision in light of the information in the record, including any information provided by the applicant, authorization holder, or licensee in response to any filings by the Executive Branch agencies.[17]

6. *Pacific Networks' and ComNet's Section 214 Authority*. Pacific Networks and ComNet are authorized to provide domestic interstate telecommunications service pursuant to blanket section 214 authority that the Commission has issued by rule.[18] Pacific Networks and ComNet each hold an international section 214 authorization.[19] Pacific Networks is authorized under its international section 214 authorization, ITC-214-20090105-00006, "to provide *resale* service in accordance with section 63.18(e)(2) on all U.S. international routes, except U.S.-China and U.S.-Hong Kong."[20] ComNet is authorized under its international section 214 authorization, ITC-214-20090424-00199, to provide "*facilities-based and resale service* in accordance with section 63.18(e)(1) and (e)(2) of the Commission's rules . . . between the United States and all permissible foreign points, except China and Hong Kong."[21] On the U.S.-China and U.S.-Hong Kong routes, both Pacific Networks and ComNet are authorized to provide switched services solely through the resale of unaffiliated U.S. facilities-based carriers' international switched services (either directly or indirectly through the resale of another U.S. resale carrier's international switched services) pursuant to section 63.18(e)(3).[22] These international section 214 authorizations are conditioned upon Pacific Networks and ComNet abiding by the commitments and undertakings set forth in their 2009 LOA to DHS and DOJ.[23]

[17] *Foreign Participation Order*, 12 FCC Rcd at 23921, para. 66 ("We emphasize that the Commission will make an independent decision on applications to be considered and will evaluate concerns raised by the Executive Branch agencies in light of all the issues raised (and comments in response) in the context of a particular application.").

[18] 47 CFR § 63.01; *see supra* para. 4 & note 10.

[19] A detailed procedural history of Pacific Networks' and ComNet's authorizations can be found in the *Order to Show Cause*. *Order to Show Cause*, 35 FCC Rcd at 3734, para. 2; *id.* at 3740-43, Appx. A, paras. 1-7.

[20] April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384 (emphasis added); *Institution Order*, 36 FCC Rcd at 6396, para. 41 (citing *Order to Show Cause*, 35 FCC Rcd at 3742-43, Appx. A, paras. 5-6; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384).

[21] May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784 (emphasis added); May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379; *Institution Order*, 36 FCC Rcd at 6396, para. 41 (citing *Order to Show Cause*, 35 FCC Rcd at 3734, para. 2; *id.* at 3740-42, Appx. A, paras. 2-4; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379; May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784). ComNet was previously named CM Tel (USA) LLC, and on March 25, 2010, the International Bureau issued a public notice of the name change. Mar. 25, 2010 Informative Public Notice, 25 FCC Rcd at 2841-42; *see Order to Show Cause*, 35 FCC Rcd at 3742, Appx. A, para. 4 (citing Mar. 25, 2010 Informative Public Notice, 25 FCC Rcd at 2841-42; Feb. 22, 2010 ComNet Letter).

[22] April 9, 2009 Grant Public Notice, 24 FCC Rcd at 4156; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379; May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784; *Institution Order*, 36 FCC Rcd at 6396, para. 41 & n.193 (citing *Order to Show Cause*, 35 FCC Rcd at 3742-43, Appx. A, paras. 5-6; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384); *id.* at 6396, para. 41 & n.195 (citing *Order to Show Cause*, 35 FCC Rcd at 3734, para. 2; *id.* at 3740-42, Appx. A, paras. 2-4; May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784).

[23] *See* April 9, 2009 Grant Public Notice, 24 FCC Rcd at 4156; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. Under the provisions of the 2009 LOA, Pacific Networks and ComNet, among other things, agree: (1) to "make . . . U.S. Records available in the United States in response to lawful U.S. process"; (2) "to provide DHS and DOJ [within 30 days after the FCC's approval of their respective . . . license applications] an up-to-date description of: [the Companies'] physical and logical technical security architecture . . . [,] their security policies and standards . . . [,] and their information technology governance controls used to oversee CM Tel's California switching facility"; (3) "to ensure that U.S. records are not made subject to mandatory destruction under any foreign laws"; (4) "to take all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in this letter"; (5) "that they will not, directly or indirectly, disclose or permit disclosure of or access to U.S. Records, Domestic Communications . . . to any person if (continued….)

7. ComNet is a Delaware limited liability company[24] that is a direct, wholly-owned subsidiary of Pacific Networks, a Delaware corporation.[25] The Companies state that ComNet and Pacific Networks are approximately 58% indirectly owned and controlled by the government of the People's Republic of China through CITIC Group Corporation,[26] a Chinese state-owned limited liability company

(Continued from previous page)
the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. government without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of DHS and DOJ or the authorization of a court of competent jurisdiction in the United States"; (6) "to maintain one or more points of contact within the United States with the authority and responsibility for accepting and overseeing compliance with a wiretap order, pen/trap order, subpoena or other lawful demand by U.S. law enforcement authorities for the content of communications or U.S. Records"; (7) "[w]ithin thirty (30) days of the event's occurrence, [the Companies] agree to notify DHS and DOJ:" (a) "if either commences the sale (or resale) of any services not described in this letter;" (b) "of any material changes in any of the facts as represented in [the 2009 LOA], or in notices or descriptions submitted pursuant to this letter;" (c) "of any material changes to their ownership structure" and "[m]aterial changes to ownership structure are those that would require a substantive transfer of control application or *pro forma* notification to the FCC, and those that would involve an increase or decrease greater than 5% in foreign government control; . . . ." (8) "Pacific Networks and CM Tel agree to negotiate in good faith with DHS and DOJ to resolve any national security, law enforcement and public safety concerns that DHS or DOJ may raise." 2009 LOA at 2-4.

[24] Pacific Networks Corp. and ComNet (USA) LLC, Response to Order Instituting Proceeding on Revocation and Termination, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199, at 46 (April 28, 2021) (PN/CN April 28, 2021 Reply) (filing with the Commission a public filing and a non-public business confidential filing); *id.*, Exh. A at A-27. In the *Institution Order*, we directed ComNet to clarify whether ComNet is a corporation or a limited liability company given discrepancies in the Commission's records. *Institution Order*, 36 FCC Rcd at 6372, para. 5, n.17; *id.* at 6415, Appx. A; *see e.g.*, 2009 LOA at 1 (identifying Pacific Networks and ComNet as "both Delaware corporations"); *but see* Pacific Networks Corp. and ComNet (USA) LLC, Response to Order to Show Cause, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199, at i, 1, 3 (June 1, 2020) (PN/CN June 1, 2020 Response) (filing with the Commission a public filing and a non-public business confidential filing) (identifying ComNet as a limited liability company, "ComNet (USA) LLC" (and formerly, "CM Tel (USA) LLC")). In their response to the *Institution Order*, the Companies state that "ComNet was formed as a limited liability company ('LLC') in 1999 [and] has remained an LLC, and thus there has been no legal change that would have required Commission notification" and clarify that "[t]he 1999 and 2009 statements cited in the [*Institution Order*] that ComNet is a 'corporation' appear to have been inadvertent misstatements." PN/CN April 28, 2021 Reply at 46.

[25] PN/CN April 28, 2021 Reply, Exh. A at A-2-A-4 (Certificate of Incorporation of Pacific Networks Corp.); *Order to Show Cause*, 35 FCC Rcd at 3734-35, para. 4, n.13; 2009 LOA at 1; Pacific Networks Corp., Application for International Section 214 Authority, File No. ITC-214-20090105-00006, Application at 2 (filed Jan. 5, 2009) (Pacific Networks 2009 Application for International Section 214 Authority).

[26] The Companies state that "the ultimate parent entity of the licensees is state-owned CITIC Group Corporation," and explain that "[a]t each link in the ownership chain, except for two, the aggregate ultimate ownership held indirectly by CITIC Group Corporation is 100%" and identify aggregate ownership percentages of 58.13% and 58.12%, respectively, held by CITIC Group Corporation in its subsidiaries, CITIC Limited and CITIC Tel. PN/CN June 1, 2020 Response at 10. Based on the Companies' filings and our assessment, the Companies are indirectly 58.13% owned and controlled by CITIC Group Corporation and thus the Chinese government. Our calculation is based on the Commission's determination of the attribution of ownership interests pursuant to Note to section 63.18(h) of its rules. 47 CFR § 63.18(h), Note to paragraph h. *See* PN/CN June 1, 2020 Response at 10 ("At each link in the ownership chain, except for two, the aggregate ultimate ownership held indirectly by CITIC Group Corporation is 100%. The two links in the ownership chain which represent less than 100% ownership by CITIC Group are: (1) the ownership by CITIC Polaris Limited and CITIC Glory Limited, each of which is a direct wholly-owned subsidiary of CITIC Group Corporation, of an aggregate of 58.13% of the equity of CITIC Limited, a publicly-traded company the stock of which is listed on the Hong Kong Stock Exchange, and (2) the ownership by Richtone Enterprises Inc., Ease Action Investments Corp., Perfect New Holdings Limited and Silver Log Holdings Ltd., each of which is an indirect controlled subsidiary of CITIC Group Corporation, of an aggregate of 58.12% of the equity of CITIC Telecom International Holdings Limited ('CITIC Tel'), a publicly-traded company the stock of
(continued….)

that is incorporated in the People's Republic of China, and which ComNet and Pacific Networks identify as their "ultimate parent."[27] According to public statements by CITIC Group Corporation, "[h]eadquartered in Beijing, CITIC Group is one of the largest Chinese conglomerates and operates both financial services and non-financial businesses in the [People's Republic of China] and internationally."[28] In the *Institution Order*, we stated that, according to Commission records, the State-owned Assets Supervision and Administration Commission of the State Council (SASAC), a Chinese government organization, directly owns 100% of CITIC Group Corporation,[29] but other publicly available information indicates that CITIC Group Corporation is funded and owned by China's Ministry of Finance.[30] In

(Continued from previous page)
which is listed on the Hong Kong Stock Exchange."); *id.* at 33-34 (describing the organizational chart attached as Exhibit A and stating, "each of those links represents over 50% ownership and therefore control" and "the links would be treated as constituting control under the Commission's rules"); *id.*, Exh. A (Pacific Networks & ComNet Organization Chart as of May 28, 2020); *id.* at ii ("an investment company owned by the People's Republic of China holds an indirect ownership interest in the Companies in excess of 50%"); *id.* at 26 ("the Chinese government's majority ownership in the Companies"); PN/CN April 28, 2021 Reply at ii ("an investment company owned by the People's Republic of China holds an indirect ownership interest in the Companies in excess of 50%"); *id.* at 43 ("The Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation"); *Institution Order*, 36 FCC Rcd at 6372-73, para. 5; *Order to Show Cause*, 35 FCC Rcd at 3734-35, para. 4.

[27] PN/CN June 1, 2020 Response, Exh. A (Pacific Networks & ComNet Organization Chart as of May 28, 2020) (referring to "CITIC Group Corporation (PRC)"); *id.* at 10 ("[T]he ultimate parent entity of the licensees is state-owned CITIC Group Corporation."); PN/CN April 28, 2021 Reply at 43; *Order to Show Cause*, 35 FCC Rcd at 3735, para. 4 & n.14; Pacific Networks Corp., Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20120126-00031, Attach. 1 at 1-2, Exhs. A, B (filed Jan. 26, 2012) (2012 Pacific Networks Pro Forma TC Notification) (stating that "CITIC Group Corporation (formerly known as CITIC Group) has taken the several restructuring actions detailed below," involving, among other things, "[t]he transformation of CITIC Group from a state-owned enterprise into CITIC Group Corporation, a state-owned limited liability company, which involved a change of the company's industrial and commercial registration . . . ."); ComNet (USA) LLC, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20120126-00030, Attach. 1 at 1-2, Exhs. A, B (filed Jan. 26, 2012) (2012 ComNet Pro Forma TC Notification) (stating that "CITIC Group Corporation (formerly known as CITIC Group) has taken the several restructuring actions detailed below," involving, among other things, "[t]he transformation of CITIC Group from a state-owned enterprise into CITIC Group Corporation, a state-owned limited liability company, which involved a change of the company's industrial and commercial registration . . . .").

[28] CITIC Group Corporation, 2018 U.S. Resolution Plan (Public Section) at 7, https://go.usa.gov/xzpTf (CITIC Group 2018 U.S. Resolution Plan). The CITIC Group 2018 U.S. Resolution Plan, as submitted to the Federal Deposit Insurance Corporation (FDIC), states that "CITIC Group is organized under the laws of the People's Republic of China" and "was founded in 1979 upon the approval of the State Council of the [People's Republic of China] (the 'State Council')." *Id.* at 1, 7. *See* Federal Deposit Insurance Corporation, *FDIC and Financial Regulatory Reform – Title I and IDI Resolution Plans* (last updated Dec. 22, 2021), https://www.fdic.gov/resources/resolutions/resolution-authority/resplans/ (explaining, "Section 165(d) of Title I of the Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA), as amended by the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA), requires certain nonbank financial companies, and bank holding companies with total consolidated assets of $250 billion or more, to submit resolution plans periodically to the FDIC, the Federal Reserve Board, and the Financial Stability Oversight Council").

[29] *Institution Order*, 36 FCC Rcd at 6372-73, para. 5 & n.19 (citing, for instance, *Order to Show Cause*, 35 FCC Rcd at 3734-35, para. 4 & n.15; 2012 Pacific Networks Pro Forma TC Notification, Attach. 1, Exh. A (identifying "Assets Supervision and Administration Commission of the State Council of China" as the government entity that "[d]irectly owns 100% of [CITIC Group Corporation]"); 2012 ComNet Pro Forma TC Notification, Attach. 1, Exh. A (identifying "Assets Supervision and Administration Commission of the State Council of China" as the government entity that "[d]irectly owns 100% of [CITIC Group Corporation]")).

[30] As stated in the *Institution Order*, other publicly available information indicates that CITIC Group Corporation is funded and owned by China's Ministry of Finance. *Institution Order*, 36 FCC Rcd at 6372-73, para. 5, n.20 (citing, (continued….)

response to the *Institution Order*, the Companies now state that the Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation without any explanation as to why they previously represented to the Commission that SASAC directly owns 100% of CITIC Group Corporation or when the change occurred.[31] As we discuss below and based on the Companies' response, the Companies either failed to file *pro forma* notifications under section 63.24(f) of the Commission's rules, which requires a filing no later than thirty (30) days after a transfer of control is completed, or, if the Ministry of Finance was always the government entity that majority-owned and controlled the Companies, filed inaccurate information in multiple filings with the Commission, and were required by the Commission's rules to correct the filings.[32]

8. *Pro Forma Notifications*. On May 12, 2021 and September 10, 2021, Pacific Networks and ComNet, respectively, filed late notifications of a *pro forma* transfer of control from a corporate restructuring that was consummated on August 27, 2014,[33] and which were required under section

(Continued from previous page)
for example, CITIC Group Corporation, *About CITIC: Corporate Governance and Risk Management*, https://www.group.citic/en/About_CITIC/Governance_Risk/ (last visited Mar. 15, 2022) (*CITIC Group Corporation Corporate Governance and Risk Management*) and quoting, "CITIC Group . . . is a conglomerate established upon the approval of the State Council. It is funded by the Ministry of Finance on behalf of the State Council.") (The *Institution Order* noted the last visited date as Mar. 16, 2021)). Given the discrepancy, we directed the Companies to clarify this ambiguity in their response to the *Institution Order*. *Institution Order*, 36 FCC Rcd at 6373, para. 5, n.20; *id.* at 6415, Appx. A.

[31] PN/CN April 28, 2021 Reply at 43; *see infra* para. 122; Pacific Networks Corp., Application for International Section 214 Authority, File No. ITC-214-20070907-00368, Attach. 2 at 4 (filed Sept. 7, 2007) (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); Pacific Networks Corp., Application for Transfer of Control of International Section 214 Authority, File No. ITC-T/C-20081219-00543, Attach. 1 at 7 (filed Dec. 19, 2008) (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); Pacific Networks 2009 Application for International Section 214 Authority, Attach. 2 at 6 (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); 2012 Pacific Networks Pro Forma TC Notification, Attach. 1, Exh. A (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); *id.*, Pacific Networks Feb. 16, 2012 Letter at 10 (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); 2012 ComNet Pro Forma TC Notification, Attach. 1, Exh. A (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); *id.*, ComNet Feb. 16, 2012 Letter at 10 (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[o]wns 100% of CITIC Group"); PN/CN June 1, 2020 Response, Business Confidential Exh. K at 4-7 (providing to DHS and DOJ a copy of the 2012 *pro forma* notifications filed with the Commission and subsequently providing corrected versions on February 16, 2012); PN/CN April 28, 2021 Reply at 77, Exh. G (attaching corrected February 16, 2012 versions of the 2012 *pro forma* notifications, which identify SASAC in the Companies' vertical line of ownership); *see* PN/CN June 1, 2020 Response, Business Confidential Exh. K at 12-16 (notifying DHS and DOJ of *pro forma* transaction in 2014, but not identifying the Chinese government organization that owns CITIC Group Corporation in the email correspondence or accompanying ownership charts).

For purposes of citations herein to Exhibit K of the Companies' June 1, 2020 response to the *Order to Show Cause*, page citations associated with Exhibit K reflect the PDF pagination of the non-public business confidential filing.

[32] 47 CFR §§ 1.65(a), 63.21(a), 63.24(f). As discussed below, the Companies had several opportunities to rectify the record throughout the pendency of this proceeding but failed to do so. *See infra* paras. 121-123.

[33] Pacific Networks Corp., Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20210512-00081 (filed May 12, 2021) (2021 Pacific Networks Pro Forma Notification); ComNet (USA) LLC, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20210910-00130 (filed Sept. 10, 2021) (2021 ComNet Pro Forma Notification) (filing two identical notifications on behalf of ComNet)
(continued….)

63.24(f) of the Commission's *pro forma* rules.[34] In the *Order to Show Cause*, the Bureaus directed the Companies to provide "an explanation as to whether certain *pro forma* transfer of control actions occurred from 2012 to 2014 concerning the subject international section 214 authorizations and whether Pacific Networks and ComNet appropriately notified the Commission, as required by the Commission's rules."[35] The Companies state that before the restructuring, the ultimate parent of the Companies, CITIC Group Corporation, "indirectly controlled more than 50% of the equity and voting power," and after the restructuring, "CITIC Group Corporation continued to indirectly control more than 50% of the equity and voting power."[36] As we discuss below, the Companies failed to comply with the Commission's *pro forma* rules and given our decision in the Order, we dismiss the Companies' pending *pro forma* notifications as moot.[37]

9. *Pacific Networks' and ComNet's Section 214 Services*. The Companies state that with regard to domestic and international services provided under section 214 authority, ComNet currently provides Wholesale International Direct Dial (IDD) Service[38] and Retail Calling Card Service,[39] and

(Continued from previous page)
(ComNet initially filed a notification on May 12, 2021, File No. ITC-T/C-INTR2021-01871, which was Dismissed by Delegated Authority on September 2, 2021); ComNet (USA) LLC, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20210910-00132 (filed Sept. 10, 2021) (ComNet withdrew a duplicate notification on Jan. 25, 2022).

[34] 47 CFR § 63.24(f).

[35] *Order to Show Cause*, 35 FCC Rcd at 3738, para. 9 & nn.30-31. In the *Institution Order*, we noted "Pacific Networks and ComNet have admitted that they are not in compliance with the Commission's rules to file *pro forma* notifications for a *pro forma* transfer of control that occurred in 2014, but have yet to cure this deficiency." *Institution Order*, 36 FCC Rcd at 6408, para. 60. The Companies did not explain the transaction with particularity in their response to the *Order to Show Cause*. In their response to the *Order to Show Cause*, the Companies state only, "[a]fter the transaction, CITIC Group Corporation continued to control over 50% of CITIC Limited, and ultimately to control over 50% of Pacific Networks and ComNet. The net result of the 2014 transfer was to replace an aggregate 100% ownership link between CITIC Group and CITIC Limited with an aggregate ownership link of 58.13%." PN/CN June 1, 2020 Response at 7. The Companies state, "[t]his transfer is discussed in the [*Order to Show Cause*]." *Id*. at 6-7 & n.19 (citing "[*Order to Show Cause*] at n.30, n.1 to Appendix B to the [*Order to Show Cause*].").

[36] *See* 2021 Pacific Networks Pro Forma Notification, Attach. at 1; 2021 ComNet Pro Forma Notification, Attach. at 1.

[37] *See infra* Section III.B.3. As discussed below, the Companies failed to explain how their ownership structure changed prior to and after the transaction that resulted in the *pro forma* transfer of control in 2014 and why such transaction was presumptively *pro forma* such as the types of transactions discussed in Note 2 of section 63.24(d) of the Commission's rules. *See* 47 CFR § 63.24(d), Note 2 to paragraph (d); 2021 Pacific Networks Pro Forma Notification, Attach. at 1; 2021 ComNet Pro Forma Notification, Attach. at 1. The Companies also failed to comply with section 63.18(h), which requires filers to provide "[t]he name, address, citizenship and principal businesses of any person or entity that directly or indirectly owns at least ten percent of the equity of the applicant, and the percentage of equity owned by each of those entities (to the nearest one percent)." 47 CFR 63.18(h); *see id.* § 63.24(f) (applying this requirement to *pro forma* notifications with respect to the assignee or transferee). The Companies did not identify the Chinese government's ownership interest in CITIC Group Corporation, and, therefore, the Companies. *See* 2021 Pacific Networks Pro Forma Notification, Attach. at 1-8; 2021 ComNet Pro Forma Notification, Attach. at 1-8.

[38] PN/CN April 28, 2021 Reply at 54-56; PN/CN June 1, 2020 Response at 13. The Companies state that "ComNet's Wholesale International Direct Dial ('IDD') service handles international voice traffic and facilitates least cost routing for carriers located in the U.S. and in foreign locations. ComNet can provide this service through traditional TDM or through IP technology via SIP. The Companies consider this service to be provided pursuant to ComNet's international [s]ection 214 authority." PN/CN April 28, 2021 Reply at 56; *see* PN/CN June 1, 2020 Response at 13. The Companies further state, with respect to ComNet's Retail Calling Card and Wholesale IDD services, that "[t]o the extent . . . that these services can facilitate domestic calls within the U.S. and a minimal
(continued….)

Pacific Networks provides "multi-protocol label switching virtual private networks ('MPLS VPN') services."[40] The Companies also state that ComNet provides other services, including: Wholesale Short Message Service (SMS); Voice over Internet Protocol (VoIP) Service; website development and hosting services; and resale of prepaid mobile data SIM cards.[41] The Companies state that with regard to ComNet's Wholesale SMS, "[a]s an information service, ComNet does not require a [s]ection 214 authorization to provide this service."[42] With regard to ComNet's VoIP service, the Companies state, "[t]he Commission has not required providers to obtain [s]ection 214 authorizations for the provision of interconnected VoIP."[43]

10. *Order to Show Cause*. On April 24, 2020, the International Bureau, Wireline Competition Bureau, and Enforcement Bureau (the Bureaus) issued the *Order to Show Cause* directing

(Continued from previous page)
amount of such calls are handled, the Companies consider these services to also be provided pursuant to ComNet's blanket domestic 214 authority." PN/CN April 28, 2021 Reply at 55.

[39] PN/CN April 28, 2021 Reply at 54-56; PN/CN June 1, 2020 Response at 14. The Companies state that "ComNet's Retail Calling Card service provides printed or digital phone cards with a set of 10-digit PIN numbers for international and domestic voice calls accessed via local or toll free numbers. As ComNet's Retail Calling Card service facilitates international calls, the Companies consider it to be provided pursuant to ComNet's international [s]ection 214 authority." PN/CN April 28, 2021 Reply at 56; *see* PN/CN June 1, 2020 Response at 14. According to the Companies, "ComNet provides Retail Calling Card service through its own calling card platform, which directly collects customer international direct dialed calls via direct inward dialing ('DID') numbers provided by local service providers, using VoIP SIP connections. End users can thus make international calls through the provided DID numbers by entering a 10-digit pin and destination number using their home or mobile phone." PN/CN April 28, 2021 Reply at 57.

[40] PN/CN June 1, 2020 Response at 12; *see* PN/CN April 28, 2021 Reply at 55. The Companies state that "Pacific Networks' MPLS VPN service provides data communications that enable its customers to operate business applications among various customer sites both within the United States and internationally." PN/CN June 1, 2020 Response at 12; PN/CN April 28, 2021 Reply at 55. The Companies state, "[w]hile Pacific Networks does not itself provide international circuits required for MPLS VPN, to the extent Pacific Networks' MPLS VPN service facilitates the exchange of international traffic, the Companies consider it to be provided pursuant to Pacific Networks' international [s]ection 214 authority." PN/CN April 28, 2021 Reply at 56. The Companies note that "[t]he Department of Justice has . . . stated that it 'is unclear that an international Section 214 authorization is required' to provide MPLS VPN services" and that they "reserve and in no way waive the argument that the MPLS VPN services provided by Pacific Networks may not, in fact, require a [s]ection 214 authorization." PN/CN June 1, 2020 Response at 13, n.33; PN/CN April 28, 2021 Reply at 55, n.109. According to the Companies, "Pacific Networks does not provide the international circuits required for international MPLS VPN," as those facilities "are purchased from unaffiliated international carriers by Pacific Networks' wholesale customer . . . and then interconnected with Pacific Networks' VPN platform in the United States." PN/CN June 1, 2020 Response at 12. The Companies state that "Pacific Networks purchases from U.S. telecommunications carriers high-speed data connections to customer locations to facilitate provision of the service." *Id*. at 12-13. To the extent the Companies "reserve" the argument that section 214 authorization is not required for Pacific Networks' MPLS VPN services, we note that the classification of services as common or private carriage is a fact-based inquiry, governed by longstanding precedents. *See, e.g., National Ass'n of Regulatory Util. Comm'rs v. FCC,* 525 F.2d 630 (D.C. Cir. 1976) (*NARUC I*); *Orloff v. FCC,* 352 F.3d 415 (D.C. Cir. 2003). Section 214 applies to the offering of telecommunications for a fee to the public at large or to such "classes of users" as to be effectively available to the public, 47 U.S.C. § 153(53); and under such precedents minor differences in price or other terms of service do not alone qualify a service as private rather than common carrier in nature. *See also National Ass'n of Regulatory Util. Comm'rs v. FCC*, 533 F.2d 601, 608-609 (1976) (describing the situations in which a carrier may be considered a common carrier).

[41] PN/CN June 1, 2020 Response at 13-15; PN/CN April 28, 2021 Reply at 54-58.

[42] PN/CN June 1, 2020 Response at 14.

[43] *Id*.

Pacific Networks and ComNet to file a response within thirty (30) calendar days demonstrating why the Commission should not initiate a proceeding to revoke and terminate their domestic and international section 214 authorizations and to reclaim ComNet's ISPCs.[44] As support, the *Order to Show Cause* referenced the Commission's 2019 *China Mobile USA Order*, in which the Commission denied the section 214 application of China Mobile International (USA) Inc. (China Mobile USA) to provide international telecommunications services between the United States and foreign destinations.[45] In the *China Mobile USA Order*, the Commission found that due to its status as a subsidiary of a Chinese state-owned entity, China Mobile USA is vulnerable to exploitation, influence, and control by the Chinese government.[46] In the *Order to Show Cause*, the Bureaus stated that the Commission's findings in the *China Mobile USA Order* raise questions regarding the vulnerability of authorization holders that are subsidiaries of a Chinese state-owned entity to the exploitation, influence, and control of the Chinese government.[47]

11. The Bureaus stated that such findings also raise questions as to the Companies' ongoing qualifications to hold domestic and international section 214 authorizations, whether retention of these authorizations and ISPC assignments by Pacific Networks and ComNet serves the public convenience and necessity, and whether ComNet's use of its ISPCs is consistent with the purpose for which they were assigned.[48] Accordingly, the *Order to Show Cause* directed the Companies to respond to certain questions concerning their ownership, operations, and other related matters.[49] The Bureaus also directed the Companies to explain "whether certain *pro forma* transfer of control actions occurred from 2012 to 2014 concerning the subject international section 214 authorizations and whether Pacific Networks and ComNet appropriately notified the Commission, as required by the Commission's rules,"[50] and to provide "a description of the extent to which Pacific Networks and ComNet are or are not otherwise subject to the exploitation, influence and control of the Chinese government."[51]

12. On June 1, 2020, the Companies filed their response to the *Order to Show Cause*, including a public filing and a non-public business confidential filing.[52] Among other arguments, the

[44] *See generally Order to Show Cause*; *see also id.*, 35 FCC Rcd at 3737, 3739, paras. 9, 11. In the *Institution Order*, we stated that Pacific Networks and ComNet provided limited information concerning ComNet's ISPCs and we asked additional questions in Appendix A of the *Institution Order*. *Institution Order*, 36 FCC Rcd at 6374, para. 8, n.29; *id.* at 6417, Appx. A.

[45] *Order to Show Cause*, 35 FCC Rcd at 3735, para. 5; *see China Mobile USA Order*, 34 FCC Rcd at 3361-62, 3380, paras. 1, 38.

[46] *China Mobile USA Order*, 34 FCC Rcd at 3365-66, para. 8.

[47] *Order to Show Cause*, 35 FCC Rcd at 3735-36, para. 6.

[48] *Id.* at 3736-37, para. 7.

[49] *Id.* at 3737-38, para. 9.

[50] *Id.* at 3738, para. 9; *see also* 47 CFR §§ 63.18, 63.24(f).

[51] *Order to Show Cause*, 35 FCC Rcd at 3738, para. 9.

[52] *See* PN/CN June 1, 2020 Response; Pacific Networks Corp. and ComNet (USA) LLC, Response to Order to Show Cause, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (June 5, 2020) (correcting non-public business confidential filing submitted on June 1, 2020); Pacific Networks Corp. and ComNet (USA) LLC, Response to Order to Show Cause, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (Jan. 12, 2022) (refiling non-public business confidential response to *Order to Show Cause* to denote where the public version of the document shows redacted information); Pacific Networks Corp. and ComNet (USA) LLC, Response to Order Instituting Proceeding on Revocation and Termination, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (Jan. 14, 2022) (filing cover letter and request for confidential treatment for resubmission of non-public business confidential response to *Order to Show Cause*); Pacific Networks Corp. and ComNet (USA) LLC, Response to Order Instituting Proceeding on Revocation and Termination, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (Jan. 18,

(continued….)

Companies contend that they are not subject to the "'exploitation, influence, and control'" of the Chinese government,[53] and they certify "under penalty of perjury" that neither company has been asked by the Chinese government or the Chinese Communist Party to take action that would jeopardize the national security and law enforcement interests of the United States.[54] They further argue that additional mitigation measures could be appropriate to address specific concerns about any security vulnerabilities.[55] To the extent that mitigation is not warranted, the Companies request that they be "given an opportunity to respond to the Bureaus' allegations at an evidentiary hearing" before an administrative law judge.[56] Additionally, they argue that the Bureaus, in the *Order to Show Cause*, do not point to specific wrongdoing that would warrant revocation.[57] They contend that adopting "the process the Commission established in the *China Mobile* [*USA*] *Order*" in the present circumstances would, in effect, be applying a new requirement for holding section 214 authorizations, and as such, the Commission should only consider the Bureaus' proposed actions through a rulemaking.[58]

13. On October 15, 2020, the International Bureau issued a letter requesting DOJ, on behalf of the Attorney General as Chair of the Committee under Executive Order 13913, to address the arguments made by the Companies in their response to the *Order to Show Cause*.[59] The letter sought "the Committee's views on Pacific Networks' and ComNet's arguments concerning whether and how they are subject to the exploitation, influence, and control of the Chinese government, and the national security and law enforcement risks associated with such exploitation, influence, and control," and asked "the Committee to respond as to whether additional mitigation measures could address any identified concerns."[60]

14. On November 16, 2020, the National Telecommunications and Information Administration (NTIA), on behalf of interested Executive Branch agencies, responded to the International Bureau's October 15, 2020 Letter and provided the views of the interested Executive Branch agencies on whether the Companies "are subject to the exploitation, influence, and control of the Chinese government, and the national security and law enforcement risks associated with such exploitation, influence, and control."[61] Among other arguments, the Executive Branch agencies contend that the same national

(Continued from previous page)
2022) (filing revised cover letter explaining that resubmission of non-public business confidential response on Jan. 12, 2022 denotes where the public versions of the documents show redacted information and clarifying correction of "Lerman Senter LLP" to "Lerman Senter PLLC" in response to *Order to Show Cause*).

[53] PN/CN June 1, 2020 Response at i, iii, 19, 24-27, 36-37.

[54] *Id.* at 19, 21, 24-25, Declaration of Li Ying (Linda) Peng.

[55] *Id*. at iii, 31-32.

[56] *Id*. at 3.

[57] *Id*. at ii; *see id.* at 27.

[58] *Id*. at 27-30.

[59] Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, to Sanchitha Jayaram, Chief, Foreign Investment Review Section, National Security Division, U.S Department of Justice at 1 (Oct. 15, 2020), 35 FCC Rcd 11493 (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199).

[60] *Id*. at 11494-95.

[61] Executive Branch Nov. 16, 2020 Letter at 2. For the purposes of the letter, the "interested Executive Branch agencies" include DOJ, DHS, DOD, Department of Commerce, Department of the Treasury, Department of State, Office of Management and Budget, Office of the U.S. Trade Representative, General Services Administration, and Council of Economic Advisers. *Id*. at 1, n.3. The letter "is not offered as a recommendation by the Committee, pursuant to Section 6 of E.O. 13913, that the FCC take any particular action with respect to the Companies" due to "the nature of the Commission's request for views on discreet [sic] factual questions, and the limited time allotted for response." *Id*. at 1.

security and law enforcement concerns that the Executive Branch raised in the China Telecom (Americas) Corporation (China Telecom Americas) and China Mobile USA recommendations[62] apply equally to Pacific Networks and ComNet.[63] The Executive Branch agencies assert that the national security environment has changed significantly since 2009—more than a decade ago—and the top threats facing the United States are different now, in view of "the culmination of years of aggressive behavior by the Chinese government and the concomitant counterintelligence challenges confronting the United States."[64] The Executive Branch agencies also state that the Chinese government's ownership and control of the Companies through CITIC Group Corporation undermines the Executive Branch agencies' confidence that additional mitigation measures would effectively address the evolved law enforcement and national security risks.[65] The Executive Branch agencies further note the statements of Congress in the June 9, 2020 Senate Permanent Subcommittee on Investigations (Senate Subcommittee) Staff Report titled, "Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers" (PSI Report).[66]

15. *Institution Order*. On March 17, 2021, we adopted the *Institution Order* to institute a proceeding to revoke the domestic authority and revoke and/or terminate the international authorizations issued to Pacific Networks and ComNet pursuant to section 214 of the Act.[67] We stated that "Pacific Networks and ComNet have failed at this stage to dispel serious concerns regarding their retention of

[62] We hereby incorporate by reference the public (i.e., redacted) versions of the following Executive Branch submissions, including the associated publicly filed exhibits in the following proceedings: *China Telecom Americas*, *China Unicom Americas*, *China Mobile USA,* and *Huawei Designation* proceedings: (1) *China Telecom (Americas) Corporation* (*China Telecom Americas*), GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate [China Telecom Americas'] International Section 214 Common Carrier Authorizations (filed Apr. 9, 2020) (Executive Branch CTA Recommendation to Revoke and Terminate); (2) *China Mobile International (USA) Inc.*; *Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, File No. ITC-214-20110901-00289, Redacted Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization (filed July 2, 2018) (Executive Branch China Mobile USA Recommendation to Deny); (3) *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket Nos. 19-351, Letter from Douglas W. Kinkoph, Associate Administrator, Office of Telecommunications and Information Applications, National Telecommunications and Information Administration, to Ajit Pai, Chairman, Federal Communications Commission (filed June 9, 2020) (NTIA Huawei June 9, 2020 Letter). All references to the foregoing submissions throughout this Order are to the public (i.e., redacted) version of the cited submission or exhibit.

[63] Executive Branch Nov. 16, 2020 Letter at 6 (citing Executive Branch CTA Recommendation to Revoke and Terminate (filing with the Commission a public filing, a non-public business confidential filing, and a classified appendix); Executive Branch China Mobile USA Recommendation to Deny (filing with the Commission a public filing, a non-public business confidential filing, and a classified appendix)); *see* Executive Branch CTA Recommendation to Revoke and Terminate at 1-7, 41 (describing changed circumstances in the national security environment, including the U.S. government's increased concern in recent years about the Chinese government's malicious cyber activities; stating that operations of a U.S. telecommunications subsidiary of a Chinese state-owned enterprise under the ultimate ownership and control of the Chinese government provide opportunities for Chinese state-sponsored actors to engage in economic espionage and to disrupt and misroute U.S. communications traffic).

[64] Executive Branch Nov. 16, 2020 Letter at 2-3; *id.* at 2-6.

[65] *Id*. at 2, 10-12.

[66] *Id*. at 2, 11 (citing Staff Report of Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, 116th Congress, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers* (June 9, 2020), https://www hsgac.senate.gov/download/threats-to-us-networks-oversight-of-chinese-government-owned-carriers (PSI Report)).

[67] 47 U.S.C. § 214; *see generally Institution Order*.

section 214 authority in the United States."[68] The *Institution Order* stated that "based on the information available in the record and consistent with the Commission's prior determination regarding risks to U.S. national security and law enforcement interests by a U.S. subsidiary of a Chinese state-owned entity, Pacific Networks and ComNet have not yet adequately demonstrated that they are not susceptible to the exploitation, influence, or control of the Chinese government."[69] The *Institution Order* further stated that "Pacific Networks and ComNet failed to fully respond to the Bureaus' questions in the *Order to Show Cause* and omitted crucial information in this proceeding that was disclosed to the Senate Subcommittee and published in the PSI Report."[70] The *Institution Order* adopted procedures allowing Pacific Networks and ComNet, interested Executive Branch agencies, and the public to present further arguments or evidence in this matter.[71]

16. *Comments*. The *Institution Order* directed the Companies to submit a filing by April 28, 2021 responding to the questions in Appendix A of the *Institution Order* and demonstrate why the Commission should not revoke and/or terminate their section 214 authority.[72] Any comments filed by the public, including the Executive Branch agencies, responding to the Response of the Companies to the *Institution Order* were due by June 7, 2021.[73] Any additional evidence or arguments filed by the Companies demonstrating why the Commission should not revoke and/or terminate their section 214 authority were due by June 28, 2021.[74] The Companies filed a response to the *Institution Order* on April 28, 2021.[75] On June 4, 2021, the Executive Branch agencies filed comments responding to certain arguments in the Companies' April 28, 2021 Reply.[76] On June 28, 2021, the Companies filed comments responding to the Executive Branch June 4, 2021 Reply.[77]

---

[68] *Institution Order*, 36 FCC Rcd at 6368-69, para. 1 (citing *China Telecom Americas Institution Order*, 35 FCC Rcd at 15006-07, paras. 1-2; *Order to Show Cause*, 35 FCC Rcd at 3735-36, para. 6; *China Mobile USA Order,* 34 FCC Rcd at 3363-64, 3365-66, 3369-70, paras. 3, 8, 17-18).

[69] *Institution Order*, 36 FCC Rcd at 6382, para. 23 (citing *China Mobile USA Order*, 34 FCC Rcd at 3361-62, 3365-66, 3368-69, paras. 1, 8, 14, 16-17; *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, 11442, paras. 46, 49; *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, Memorandum Opinion and Order, PS Docket No. 19-351, 35 FCC Rcd 14435, 14440-41, paras. 16-17 (2020) (*Huawei Designation Order*)).

[70] *Institution Order*, 36 FCC Rcd at 6404, para. 52.

[71] *Id*. at 6369, para. 1.

[72] *Id*. at 6414, para. 75.

[73] *Id*.

[74] *Id*.

[75] *See* PN/CN April 28, 2021 Reply. On April 16, 2021, Pacific Networks and ComNet filed a motion for an extension of the time for their response to the *Institution Order* until May 12, 2021, and ultimately filed their response by the original due date of April 28, 2021. Pacific Networks Corp. and ComNet (USA) LLC, Motion for Extension, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (filed April 16, 2021).

[76] *See* Letter from Kathy Smith, Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau (June 4, 2021) (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199) (Executive Branch June 4, 2021 Reply).

[77] *See* Pacific Networks Corp. and ComNet (USA) LLC, Response to NTIA Letter, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (June 28, 2021) (PN/CN June 28, 2021 Reply). On January 13, 2022, the Companies filed an *ex parte* letter. Letter from Jeffrey J. Carlisle, Counsel to Pacific Networks Corp. and ComNet (USA) LLC, Lerman Center PLLC, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (filed Jan. 13, 2022) (PN/CN *Ex Parte* Letter).

III. DISCUSSION

17. After providing the Companies several opportunities to respond with their own evidence and make any factual or legal arguments contending otherwise, we find, based on our public interest analysis under section 214 of the Act and the totality of the extensive record evidence, that the present and future public interest, convenience, and necessity is no longer served by the Companies' retention of their section 214 authority. *First*, we discuss the Commission's standard of review and how the procedures adopted in this proceeding comply with constitutional and statutory requirements and are consistent with Commission policy and precedent. In doing so, we reject the Companies' contentions that "the further process created by the [*Institution Order*] is an illusion of fair process" and "the Commission has ignored or waved away numerous protections that have long been the hallmarks of the Commission's process."[78] *Second*, we discuss the overwhelming record evidence supporting our revocation of the Companies' domestic section 214 authority, and our revocation and termination of their international section 214 authorizations. *Third*, we discuss our finding that further mitigation will not address the substantial and unacceptable national security and law enforcement concerns. *Finally*, we discuss the transition period during which Companies must discontinue all services they provide under their section 214 authority.

A. Standard of Review

1. Applicable Standard of Proof and Burden of Proof

18. Consistent with applicable law and the Supreme Court's decision in *Steadman v. SEC*, we use the preponderance of the evidence as the standard of proof in reviewing the full record to determine whether revocation of the Companies' domestic section 214 authority and revocation and termination of their international section 214 authorizations is warranted.[79] We are unpersuaded by the Companies' arguments that the more appropriate standard is the "clear and convincing evidence" standard articulated in *Sea Island Broadcasting Corp. of S.C. v. FCC*.[80] In that case, the D.C. Circuit concluded that "revocation of an FCC [broadcast] license is governed, at the agency level, by the 'clear and convincing' standard of proof," the same standard that the court had applied to the SEC's revocation of a broker's license in *Collins Securities Corp. v. SEC*.[81] The Companies assert that *Steadman* did not change this particular standard for revocation "especially where, as here, revocation would destroy the Companies' livelihood in the U.S. that was established under permanent [s]ection 214 authorizations."[82] As support, the Companies cite *SEC v. Moran* for the proposition that the clear and convincing standard applies when a defendant in an administrative proceeding faces a judgment that "could potentially impose penalties such as loss of liberty, deportation, termination of parental rights, or *deprivation of ability to engage in*

[78] PN/CN April 28, 2021 Reply at 24. In particular, for the reasons described in this Order, we reject the Companies' arguments that the Commission chose a less stringent standard of proof than the law requires and shifted the burden of proof to the Companies, expanded the grounds justifying revocation of section 214 authority, refused to acknowledge that material facts are in dispute, refused to hold an evidentiary hearing, refused to provide the expert Executive Branch agencies sufficient time for input, proceeded without a recommendation from those expert agencies, refused to review any of the procedural or substantive questions raised in a rulemaking, and refused to assess whether any of the risks it has identified could be mitigated. *Id.* at ii-iii, 28-29.

[79] *Steadman v. SEC,* 450 U.S. 91, 101 & n.21 (1981) (citing *Sea Island Broadcasting Corp. of S.C. v. FCC,* 627 F.2d 240, 243 (D.C. Cir. 1980)); *James A. Kay, Jr.*, Decision, 17 FCC Rcd 1834, 1837, para. 11 (2002) (subsequent history omitted).

[80] PN/CN April 28, 2021 Reply at 25 (citing *Sea Island*, 627 F.2d at 244).

[81] *Sea Island*, 627 F.2d at 244 (holding that revocation of a license to operate an AM radio station was governed, at the agency level, by the "clear and convincing" standard of proof set forth in the *Collins* decision, rather than the "preponderance of evidence" standard that the Commission had applied in revoking the AM license) (citing *Collins Securities Corp. v. SEC,* 562 F.2d 820 (D.C. Cir. 1977), *abrogated by Steadman*, 450 U.S. at 95).

[82] PN/CN April 28, 2021 Reply at 25.

one's *livelihood*."[83] The Companies contend that such would be the case here as "the Commission is seeking to permanently bar the Companies from being able to provide [s]ection 214 services."[84]

19. As we stated in the *China Unicom Americas Order on Revocation* and the *China Telecom Americas Order on Revocation and Termination*, "in the absence of any statutory requirement to the contrary, the standard of proof governing administrative hearings is the well-established preponderance of the evidence standard, and not clear and convincing evidence—even in formal administrative hearings required by statute to be conducted on the record."[85] The Supreme Court clearly held in *Steadman* that the standard of proof for adjudicatory proceedings subject to the Administrative Procedure Act (APA)—which is the case here—is the "preponderance of the evidence," thereby eliminating the rationale for the D.C. Circuit's opinion in *Sea Island*.[86] The Court also explicitly abrogated the *Collins* decision, cited in *Sea Island*, in which the D.C. Circuit held that SEC action resulting in deprivation of livelihood required application of the clear and convincing evidentiary standard.[87] As such, the Companies' continued reliance on *Sea Island* is itself misplaced. Moreover, *dicta* in *SEC v. Moran*, a decision by the District Court for the Southern District of New York, does not alter our view regarding the appropriate standard of proof in the revocation of section 214 authority. Indeed in *Moran,* the District Court held that the appropriate standard of proof under the facts presented was the preponderance of the evidence and not clear and convincing evidence.[88]

20. The Companies also argue that despite Commission precedent that "makes clear that the Commission and the Bureaus bear the burden of proof when seeking to revoke a license or authorization,"[89] the *Institution Order* has "[placed] the burden of proof in this proceeding on the Companies by requiring them to prove the negative proposition that they are not subject to exploitation by a foreign state."[90] We disagree with the Companies' contention that we are requiring them to prove a

[83] *Id.* at 25-26 (quoting *SEC v. Moran*, 922 F. Supp. 867 (S.D.N.Y. 1996) (emphasis added)).

[84] *Id.* at 26. Pacific Networks and ComNet also argue that "*Sea Island Broadcasting* held renewable licenses and could hold or acquire other broadcast licenses" and that "[i]f the Commission applied the 'clear and convincing' standard in Sea Island Broadcasting based on those consequences, it certainly must do so here where the jeopardy is even greater." *Id*.

[85] *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 26; *China Telecom Americas Order on Revocation and Termination* at *5, para. 15.

[86] *Steadman v. SEC*, 450 U.S. at 104; *see China Unicom Americas Order on Revocation*, FCC 22-9 at para. 26; *China Telecom Americas Order on Revocation and Termination* at *5, para. 15, n.57.

[87] *Steadman*, 450 U.S. at 95 (abrogating *Collins Securities Corp. v. SEC,* 562 F.2d 820); *see also Sea Island*, 627 F.2d at 244 (holding that *Collins* standard for revocation of a broker's license applied to revocation of an FCC broadcast license).

[88] *Moran*, 922 F. Supp. at 890 (finding, based on the facts of the case, that "this case shall be governed by the preponderance of the evidence standard").

[89] PN/CN April 28, 2021 Reply at 24 (citing *Kintzel Order*, 22 FCC Rcd at 17207, para. 28, *case terminated by consent*, FCC 09M-52 (ALJ 2009); *NOS Communications, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6952, 6965, para. 28 (2003) (*NOS Communications Order*), *case terminated by consent*, FCC 03M-42 (ALJ 2003); *Business Options, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6881, 6894, para. 37 (2003) (*Business Options Order*), *case terminated by consent*, 19 FCC Rcd 2916 (2004) (attaching *Consent Order,* FCC 04M-08 (ALJ 2004)); *Publix Network Corporation, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 17 FCC Rcd 11487, 11508, para. 47 (2002) (*Publix Order*), *Consent Order*, FCC 05M-12 (ALJ 2005); *CCN, Inc. Order to Show Cause*, 12 FCC Rcd at 8561, para. 24; *CCN, Inc. Order*, 13 FCC Rcd 13599).

[90] PN/CN April 28, 2021 Reply at 24. The Companies also state that the *Order to Show Cause* "placed the burden on the Companies to show why a revocation proceeding should not be initiated, and in the very first paragraph of the [*Institution Order*] the Commission states that the Companies 'have failed at this stage to dispel serious concerns regarding their retention of [s]ection 214 authority.'" *Id*. (citing *Institution Order*, 36 FCC Rcd at 6368, para. 1).

(continued….)

negative proposition. As we discuss below, given the concerns raised in the *Order to Show Cause* and *Institution Order*, the Companies could have offered evidence of laws or procedures that would allow them to resist the demands of the Chinese government or Chinese Communist Party, but they have failed to do so.[91]

2. Public Interest Standard

21. We reject Pacific Networks' and ComNet's contention that revocation of a license or authorization is reserved for "a narrow set of cases involving serious misconduct or abuse."[92] The Companies claim that "the Commission's discretion to revoke [a section 214] authorization lies only in cases of adjudicated misconduct,"[93] which is "a violation of the terms of an authorization, the [Communications] Act, or a Commission rule or order."[94] The Companies further state that "[i]n rejecting this precedent, the [*Institution Order*] does not cite any contrary interpretation, aside from a different recent case involving a state-owned Chinese company" and that the Commission "asserts, notwithstanding its past precedent, that it is now 'unreasonable' to conclude serious misconduct could be the only reason for revocation, and fails to provide any limiting principle . . . [to] the rather broad rule that it must evaluate 'all aspects of the public interest.'"[95]

22. We affirm our prior determination in the *Institution Order* and related proceedings that it is unreasonable to conclude that serious misconduct or abuse could be the only justification for revocation, as the Companies assert, given the Commission's ongoing responsibility to evaluate all aspects of the public interest, including national security and law enforcement concerns.[96] Indeed, while section 312 of the Act does not apply here, it permits revocation of Title III licenses and permits based on a number of other grounds, including "conditions coming to the attention of the Commission which would warrant it in refusing to grant a license or permit on an original application."[97] As we stated in the *China Unicom Americas Order on Revocation* and the *China Telecom Americas Order on Revocation and Termination*, "[t]he same principle applies to determinations of the public convenience and necessity under section 214 of the Act where the Commission has reserved its 'authority to enforce our safeguards through . . . the revocation of authorizations'[] and explained that it grants 'blanket' and 'global' authorizations with the understanding that they may be revoked."[98] Further, as the Commission

(Continued from previous page)
We note that directing the Companies to demonstrate why their authorizations should not be revoked is consistent with prior Commission orders directing relevant parties to similarly show cause why their section 214 authority should not be revoked. *See Kintzel Order*, 22 FCC Rcd at 17205, para. 24; *NOS Communications Order*, 18 FCC Rcd at 6964, para. 25; *Business Options Order*, 18 FCC Rcd at 6893, para. 34; *Publix Order*, 17 FCC Rcd at 11506, para. 44; *CCN, Inc. Order to Show Cause,* 12 FCC Rcd at 8560, para. 21.

[91] *See infra* paras. 45, 67.

[92] PN/CN April 28, 2021 Reply at 26 (citing PN/CN June 1, 2020 Response at 19; *Domestic 214 Blanket Authority Order*, 14 FCC Rcd at 11374, para. 16 (stating when adopting blanket domestic section 214 authorizations "the Commission will still be able to revoke a carrier's section 214 authority when warranted in the relatively rare instances in which carriers abuse their market power or their common carrier obligations")).

[93] *Id.* at 36 (citing *Foreign Participation Order*, 12 FCC Rcd at 24022 [sic], para. 295).

[94] *Id.* (citing *Marpin Telecoms and Broadcasting Co. Ltd. v. Cable & Wireless, Inc.*, 18 FCC Rcd 508, 515 (2003)).

[95] *Id.* at 26-27 (citing *Institution Order*, 36 FCC Rcd at 6381-82, para. 21).

[96] *Institution Order*, 36 FCC Rcd at 6381, para. 21; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 28; *China Telecom Americas Order on Revocation and Termination* at *6, para. 17; *see* PN/CN April 28, 2021 Reply at 26, 36.

[97] 47 U.S.C. § 312(a)(2); *see generally* 47 U.S.C. § 312.

[98] *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 28 (citing *Domestic 214 Blanket Authority Order*, 14 FCC Rcd at 11372-73, 11374, paras. 12-14, 16; *Personal Communications Industry Association's Broadband Personal Communications Services Alliance's Petition for Forbearance for Broadband Personal*
(continued….)

concluded in the *CCN, Inc. Order*, section 4(i) of the Communications Act also supports revocation authority, as reasonably ancillary to the Commission's authority to authorize common carrier service in the first instance.[99] We therefore find that revocation based upon an assessment of the public interest, convenience, and necessity under section 214 of the Act may be based on other public interest factors coming to the attention of the Commission, including factors that may not be under the carrier's control.[100]

3. The Companies Had Sufficient Notice and Several Opportunities to Be Heard

23. We find that the procedures we adopted in this proceeding are consistent with principles of due process, applicable law, and the Commission's policy and precedent, and provided the Companies with sufficient notice and several opportunities to be heard. Accordingly, we reject the Companies' arguments that the process here conflicts with the Due Process Clause and APA requirements; the Commission cannot serve as a neutral fact finder; the procedures are inconsistent with the Commission's rules, policy, and precedent; and the Commission improperly avoids an evidentiary hearing as material facts are in dispute.[101]

a. Procedures Comply with Due Process Requirements and the APA

24. At the outset, we decline to address the Companies' arguments that their section 214 authorizations are a "protected interest" because they "had a reasonable expectation that absent material changes in the authorization, the authorization would continue to be effective indefinitely,"[102] and that "[a]s a protectable interest, the U.S. Constitution requires 'basic fairness' and 'procedures reasonably designed to protect against erroneous deprivation of' a party's interests."[103] As we stated in a related proceeding, "[w]e assume, without deciding, that foreign-owned carriers' interest in retaining section 214 authority to operate communications networks in the United States is entitled to due process protection."[104]

(Continued from previous page)
Communications Services, Memorandum Opinion and Order, 13 FCC Rcd 16857, 16881, para. 48 (1998) ("[W]e find that it is necessary to continue to require that international services be provided only pursuant to an authorization that can be conditioned or revoked.")); *China Telecom Americas Order on Revocation and Termination* at *6, para. 17 (same).

[99] 47 U.S.C. § 154(i); *CCN, Inc. Order*, 13 FCC Rcd at 13607, para. 12; *see also China Unicom Americas Order on Revocation*, FCC 22-9 at para. 22.

[100] *See China Unicom Americas Order on Revocation*, FCC 22-9 at para. 28; *China Telecom Americas Order on Revocation and Termination* at *6, para. 17.

[101] *See* PN/CN April 28, 2021 Reply at 2-3, 26-43. Among other things, Pacific Networks and ComNet also claim that "the Commission is willing to ignore or reverse any possible procedural or evidentiary constraint to reach a pre-ordained conclusion." *Id*. at 29. We disagree. As discussed in this Order, we find that the procedures we adopted in this proceeding comply with constitutional and statutory requirements and are consistent with Commission policy and precedent. *See infra* Section III.A.3.a.

[102] PN/CN April 28, 2021 Reply at 36 (citing, for example, *Spinelli v. New York*, 579 F.3d 130 [sic], 168-69 (2009) (holding that a granted business license is a protected property interest requiring due process); *3883 Conn. LLC v. Dist. of Columbia*, 336 F.3d 1068, 1072 (D.C. Cir. 2003)).

[103] PN/CN April 28, 2021 Reply at 37 (citing *Al Haramain Islamic Found, Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 980 (9th Cir. 2012)).

[104] *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 30; *see Institution Order*, 36 FCC Rcd at 6379, para. 17, n.68; *id*. at para. 17 (" . . . the process we outline [in the *Institution Order*] is sufficient to resolve the ultimate questions in most section 214 cases while providing carriers with due process.").

25. The Companies contend that due process here "warrants a hearing before the Companies are deprived of their protectable interests in the [s]ection 214 authorization"[105] and that our "refusal to afford [them] the procedural protections usually afforded in revocation proceedings, with a minimum of explanation in the [*Institution Order*], is arbitrary, capricious and an abuse of discretion, and separately denies [them] their rights to due process."[106] We have afforded the Companies ample opportunity to be heard and raise any factual or legal arguments in this matter. We are not required to conduct the additional evidentiary hearing procedures the Companies claim are warranted. The Supreme Court has held that "the ordinary principle [is] that something less than an evidentiary hearing is sufficient prior to adverse administrative action."[107] As we stated in related cases, the procedural requirements for formal adjudications under the APA[108] do not apply here,[109] and live evidentiary hearings are the rare exception rather than the norm.[110] Courts have held that the question of whether to hold an evidentiary hearing is "within [the agency's] discretion, and it may 'properly deny an evidentiary hearing if the issues, even disputed issues, may be adequately resolved on the written record, at least where there is no issue of motive, intent or credibility.'"[111]

26. Contrary to the Companies' assertion that the process established here "prejudices the Companies by denying them an opportunity to be heard and 'fair processing of an action,'"[112] we conclude that the ultimate decisions about revocation in this case may be resolved on the present record. The Companies have had several opportunities to respond to the Commission's concerns, beginning with the *Order to Show Cause*.[113] The *Institution Order*, in turn, provided the Companies with a "further opportunity" to explain why "the *present and future* public interest, convenience, and necessity is served by their retention of their domestic and international section 214 authorities and why the Commission should not revoke their domestic authority and revoke and/or terminate their international section 214 authorizations."[114] Moreover, contrary to the Companies' assertion that the *Mathews v. Eldridge* "factors

[105] PN/CN April 28, 2021 Reply at 37 (citing, for example, *Zinermon v. Burch*, 494 U.S. 113, 132 (1990) (requiring a predeprivation hearing where feasible)).

[106] *Id.* at 23.

[107] *Mathews v. Eldridge*, 424 U.S. 319, 343 (1976); *see China Unicom Americas Order on Revocation*, FCC 22-9 at para. 32; *China Telecom Americas Order on Revocation and Termination* at *9, para. 24; *Institution Order*, 36 FCC Rcd at 6379-80, para. 17; *China Unicom Americas Institution Order*, 36 FCC Rcd at 6330-31, para. 19.

[108] *See* 5 U.S.C. §§ 554, 556, and 557; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 32; *China Telecom Americas Order on Revocation and Termination* at *9, para. 24.

[109] *See Procedural Streamlining of Administrative Hearings*, Report and Order, 35 FCC Rcd 10729, 10731-32, para. 9, n.24 (2020) (*Administrative Hearings Order*) (citing *United States v. Florida East Coast Railway Co.*, 410 U.S. 224, 234-38 (1973)); *Empresa Cubana Exportada de Alimentos y Productos Varios v. U.S. Dep't of Treasury*, 638 F.3d 794, 802 (D.C. Cir. 2011).

[110] *See China Unicom Americas Order on Revocation*, FCC 22-9 at para. 32; *China Telecom Americas Order on Revocation and Termination* at *9, para. 24.

[111] *NRG Power Mktg., LLC v. FERC*, 718 F.3d 947, 959 (D.C. Cir. 2013) (quoting *Pac. Gas & Elec. Co. v. FERC*, 306 F.3d 1112, 1119 (D.C. Cir. 2002)). Even questions of intent do not necessarily require trial-type hearings, where no basis has been advanced for challenging a party's assertion as to its intent. *See Minisink Residents for Envtl. Pres. & Safety v. FERC*, 762 F.3d 97, 114-15 (D.C. Cir. 2014) (holding that FERC properly resolved an issue of intent on a written record). *See also China Unicom Americas Order on Revocation*, FCC 22-9 at para. 32; *China Telecom Americas Order on Revocation and Termination* at *9, para. 24.

[112] PN/CN April 28, 2021 Reply at 36 (citing *United States v. Morgan*, 193 F.3d 252, 267 (1999) (quoting *Garcia-Flores*, 17 I. & N. Dec. 325, 329 (BIA 1980))).

[113] *See generally Order to Show Cause*; *see also Institution Order*, 36 FCC Rcd at 6374, para. 8.

[114] *Institution Order*, 36 FCC Rcd at 6377, para. 13.

weigh in favor of providing the Companies with a live hearing,"[115] we find that the procedures we adopted are consistent with the three-factor *Mathews* test: (1) "the private interest that will be affected by the official action;" (2) "the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards;" and (3) "the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail."[116]

27. With regard to the first factor, Pacific Networks and ComNet state that revocation of their section 214 authority would, among other things, (1) "eliminate the Companies' ability to continue to provide telecommunications services to customers in the U.S. on a common carrier basis,"[117] (2) "cripple their businesses and likely result in employees in the U.S. losing their jobs at a time of considerable economic uncertainty,"[118] and (3) "damage . . . [their] reputation . . . and their employees . . . [as] officially branding any company as a risk to national security would permanently stain the reputation of the Companies and their employees."[119] Thus, according to the Companies, the "impact of a revocation on the interests of the Companies and its [sic] employees are . . . extensive and weigh heavily in favor of a neutral finder of fact reviewing the record."[120] We disagree. Although we recognize that revocation will have an impact on the Companies and their customers, private companies have no unqualified right to operate interstate transmission lines—on the contrary, Congress has conditioned such activity on a showing that it would serve the "public convenience and necessity."[121] Thus, section 214 of the Communications Act puts regulated entities on notice that authorizations may be revoked if they are no longer in the public interest. Significantly, national security and law enforcement needs have been an express focus of that public interest requirement since at least 1997, well before the Companies obtained their section 214 authority.[122]

28. With regard to the second *Mathews* factor, the Companies have not shown the value of any additional process or how it would prevent erroneous deprivation, and we therefore find that the procedures that the Commission followed satisfy the bedrock requirements of due process—notice and

[115] The Companies note that "in 2020, the Commission explained in the Administrative Hearings Order when due process requires an evidentiary hearing, and in such instances applying the three-part test the Supreme Court adopted in [*Mathews v. Eldridge*]." PN/CN April 28, 2021 Reply at 30-31 (citing *Administrative Hearings Order*, 35 FCC Rcd at 10733, para. 12; *Mathews v. Eldridge*, 424 U.S. at 335).

[116] *Mathews*, 424 U.S. at 335; *cf. Administrative Hearings Order*, 35 FCC Rcd at 10733, para. 12 ("[t]o determine whether due process requires live testimony is a particular case, the presiding officer will apply the three-part test the Supreme Court adopted in *Mathews v. Eldridge*").

[117] PN/CN April 28, 2021 Reply at 31. Pacific Networks and ComNet state they "have built a business that provides service to hundreds of thousands of users of retail calling cards, millions of minutes of carriage to service providers using Wholesale IDD, and efficient intracompany communications to companies using MPLS VPN." *Id*.

[118] *Id.*

[119] *Id*.

[120] *Id*. at 31-32.

[121] 47 U.S.C. § 214(a). It is especially unlikely that a company majority-owned and controlled by a foreign government can claim that its private interests weigh substantially against this statutory "public convenience and necessity" condition. Although foreign government control of a U.S. carrier in and of itself is not grounds for depriving it of an international section 214 application, the Commission has made clear that national security, law enforcement, and foreign policy considerations are considered independently of other factors and are not subject to the general presumption in favor of entry. *See Foreign Participation Order*, 12 FCC Rcd at 23920-21, para. 65; *China Mobile USA Order*, 34 FCC Rcd at 3371-72, para. 20 & n.63; *see also China Telecom Americas Order on Revocation and Termination* at *10, n.124; *China Unicom Americas Order on Revocation*, FCC 22-9 at n.130.

[122] *See*, *e.g.*, *Foreign Participation Order*, 12 FCC Rcd at 23919-21, paras. 61-66.

the opportunity to be heard "at a meaningful time and in a meaningful manner."[123] The Companies argue that: (1) the "factual conclusions" in the *Institution Order*, based on the written record to date, rely almost entirely on hypotheticals, inference, and potential implications rather than factual evidence, and (2) the *Institution Order* made "unwarranted conclusions about the Companies' transparency without the Commission seeking clarification, and failed to correctly characterize the one service it analyzed."[124] The Companies contend this demonstrates that the "risk of 'erroneous deprivation' is and will continue to be significant and merits 'additional or substitute procedural safeguards' to evaluate material facts, not 'further proceedings' that simply continue to limit the Companies' procedural protections."[125] We are not persuaded by these contentions as we discuss in this Order.[126] The Companies have not explained why the process the Commission afforded them, in which the Companies submitted several rounds of written comments to respond to the specific bases for revocation proposed in the *Order to Show Cause* and the *Institution Order*, does not provide them a meaningful opportunity to present their case. Nor have they identified any material factual issues in dispute that would warrant an evidentiary hearing, as opposed to questions subject to the Commission's predictive judgment based on the record in this proceeding.[127] Neither the APA nor the Communications Act requires the conduct of formal evidentiary hearings in this matter,[128] and we find that it is more than sufficient due process in this context to provide Pacific Networks and ComNet with timely and adequate notice of the reasons for revocation; opportunity to respond with their own evidence and to make any factual, legal, or policy arguments; access to the

[123] *See, e.g., Mathews*, 424 U.S. at 333 (citing *Armstrong v. Manzo*, 380 U.S. 545, 552 (1965)); *cf.* 5 U.S.C. § 558(c)(1)-(2) (permitting "revocation . . . of a license" following "notice by the agency in writing" of any basis for revocation and an "opportunity to demonstrate compliance").

[124] PN/CN April 28, 2021 Reply at 32.

[125] *Id*.

[126] *See generally infra* Section III.

[127] *See generally infra* Sections III.A.3.c., III.B., III.C., III.D.

[128] *See Administrative Hearings Order*, 35 FCC Rcd at 10732, para. 9 ("Where an agency's enabling statute does not expressly require an 'on the record' hearing and instead calls simply for a 'hearing,' a 'full hearing,' or uses similar terminology, the statute does not trigger the APA formal adjudication procedures absent clear evidence of congressional intent to do so."); *United States v. Florida East Coast Railway Co.*, 410 U.S. at 234-38 (the words "after hearing" in the Interstate Commerce Act do not require formal APA adjudication); *see also, e.g*., *City of West Chicago, Ill. v. U.S. Nuclear Regulatory Comm'n*, 701 F. 2d 632, 641 (7th Cir. 1983) (statutory requirement of a "hearing" does not trigger formal, on-the-record hearing provisions of the APA); *Chem. Waste Mgmt., Inc. v. EPA*, 873 F.2d 1477, 1480-83 (D.C. Cir. 1989) (no presumption that "public hearing" means "on the record" hearing); *Farmers Union Cent. Exch. v. FERC*, 734 F.2d 1486, 1499 n.39 (D.C. Cir. 1984) ("after full hearing" is "not equivalent to the requirement of a decision 'on the record"') (internal citation omitted).

evidence the Commission considers;[129] a written order from the Commission providing its preliminary reasoning; and opportunity to respond to the Commission's preliminary findings.[130]

29. The third *Mathews* factor—the fiscal and administrative burden on the Government—weighs heavily in favor of the Commission. As we observed in the *China Unicom Americas Order on Revocation* and the *China Telecom Americas Order on Revocation and Termination*, courts have recognized that hearings before an administrative law judge, with live testimony and cross examination, impose significant temporal and cost burdens on agencies.[131] The burden on the government would be especially heavy in this case, as a trial before an administrative law judge could require national security officials to take time away from their essential duties to participate in additional administrative proceedings.[132] More importantly, given the national security issues at stake, any resulting unwarranted delay could be harmful.[133] Additionally, we are not persuaded by the Companies' argument that the Commission has failed to show "the fiscal or administrative burdens would outweigh the other two parts" because the *Mathews* test "does not allow an agency to ignore the need for a hearing based on the existence of *any* burden more significant than that of the current process."[134] In this case, we have determined that the first two *Mathews* factors weigh in favor of the Commission. As such, the Companies' argument that the *Institution Order* failed to show that "the burden is disproportionate to the need for a hearing as demonstrated by the first two parts" is incorrect.[135] And the Companies have given us no reason here to believe that live testimony would shed meaningful light on material facts.[136] Thus,

[129] The Companies argue that they "have never seen documents cited by the PSI Report, and which the [*Institution Order*] cites . . . . Thus, contrary to the [*Institution Order's*] assertion that the Companies have access to all of the materials they need, and that discovery is not necessary, the Companies in fact have not had access to materials cited in the PSI Report that have now been relied on by the Commission." PN/CN April 28, 2021 Reply at 40-41. We reject the Companies' argument that additional process, to include discovery, is necessary here. As a general matter, the Commission is not relying on anything that the Companies cannot access. With regard to the PSI Report, the Commission only relied on the public-facing part of the PSI Report, which the Companies can similarly access. The Commission did not have access to or otherwise rely on the underlying materials that are cited in the PSI Report. Indeed, the Companies provided responses to the Senate Subcommittee and possess the information relevant to this proceeding. As discussed below, rather than provide the Commission with the same information they submitted to the Senate Subcommittee to the Commission, the Companies instead omitted crucial information in their response to the *Order to Show Cause* and provided us with evasive responses and non-answers to our information requests in the *Order to Show Cause* and the *Institution Order*.

[130] *See Louisiana Ass'n of Indep. Producers & Royalty Owners v. FERC*, 958 F.2d 1101, 1114 (D.C. Cir. 1992) (rejecting due process challenge to lack of a hearing and holding that petitioners had a meaningful opportunity to be heard before the Federal Energy Regulatory Commission where they received notice of and opportunity to review evidence, a chance to submit briefs criticizing the evidence and to submit new evidence, and to argue before the full Commission).

[131] *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 35 (citing, for example, *Chem. Waste Mgmt.,* 873 F.2d at 1485; *G.E. v. EPA*, 595 F. Supp. 2d 8, 38-39 (D.D.C. 2009)); *China Telecom Americas Order on Revocation and Termination* at *10, para. 27 (same).

[132] *See Mathews*, 424 U.S. at 347-49.

[133] *See, e.g., California ex rel. Lockyer v. FERC*, 329 F.3d 700, 711, 713 (9th Cir. 2003) (agency has a strong interest in reaching a decision at the earliest practicable time when delay could endanger the agency's administrative mission by preventing it from acting to mitigate harm).

[134] PN/CN April 28, 2021 Reply at 32-33.

[135] *Id.* at 33.

[136] Pacific Networks and ComNet also note the Commission's statement in the *Institution Order* that the "fiscal and administrative burden of such additional process *could* be quite substantial and disruptive if it were to involve participation by Commission staff or officials from other agencies in oral proceedings." *Id.* at 32 (citing *Institution Order*, 36 FCC Rcd at 6379-80, para. 17 (emphasis added)). The Companies argue that "[t]his implies that

(continued….)

our *Mathews* analysis supports our conclusion that no live evidentiary hearing is required and that the process afforded to Pacific Networks and ComNet here has been sufficient. Even if the Companies have some cognizable private interest here, any such interest is substantially outweighed by the extensive process that we have followed, our conclusion that there would be little or no benefit from receiving live witness testimony, and the fiscal, administrative, and national security interests that would be harmed by further delay of the government's resolution of this important matter.

30. We also reject the Companies' separate contention that the *Institution Order's* process conflicts with the APA.[137] As discussed herein, the procedures we followed in this proceeding are consistent with Commission policy and precedent as well as the APA.[138] To the extent they can be construed as deviating from such policy and precedent, we explain in this Order the bases for any such perceived deviations.[139]

b. The Commission Can Serve as a Neutral Fact Finder

31. We find that the Commission can serve as a neutral fact finder contrary to the Companies' claims. Specifically, the Companies claim that the process we adopted prejudices [them] by "the Commission's failure to administer its rules in a consistent fashion and provide [them] with a full and fair hearing before a neutral arbitrator."[140] The Companies argue that the *Institution Order* "shows a willingness to interpret every fact against the Companies, and to ignore every piece of evidence of the Companies' compliance with Commission regulations and the 2009 Letter of Assurance," that "[t]he Commission took no opportunity over the ten months that it had [the Companies' Response to the *Order to Show Cause*] to reach out to [them] and clarify any of the alleged discrepancies or omissions, instead reserving them to bolster its case for revocation[,]"[141] and that"[t]he results from other cases also indicate an unwillingness on the part of the Commission to consider any mitigating facts contrary to its

(Continued from previous page)
'participation [is] needed in this proceeding to reach a fair conclusion' and that 'multiple sources could weigh in on material facts at issue in this case.'" *Id*. at 33. The Companies also assert that "[t]o the extent the Commission attempts to rely on an opinion or statement regarding disputed issues of material fact . . . such opinion or statement should be subject to review and dispute by the Companies using substantiated evidence. An oral proceeding is necessary to ensure that the Companies are presented with the evidence held against them and have an adequate opportunity to rebut it." *Id*. Again we reject these argument for the reasons described herein. *See generally infra* Sections III.A.3.c., III.B., III.C., III. D.

[137] PN/CN April 28, 2021 Reply at 34-35 (citing 5 U.S.C. § 706(2)(A); *United States v. Bean*, 537 U.S. 71, 77 (2002)). The Companies state that "the Supreme Court has restricted review of agency action for abuse of discretion when the authorizing statute is "drawn in such broad terms that in a given case there is no law to apply." *Id*. at 35 (citing *Citizens to Preserve Overton Park v. Volpe*, 401 U.S. 402, 410 (1971)). The Companies also contend that the process adopted in the *Institution Order* "would likely be set aside as impermissibly arbitrary, capricious and an abuse of discretion [as] [t]he list of unilateral and unannounced changes to policy the Commission has had to adopt within this adjudicatory proceeding—in some cases with little to no reasoned discussion—is substantial, and the Commission will be put in the position of having to defend each one of those decisions, both individually and in the aggregate effect they have on the overall fairness of this proceeding." *Id*.

[138] *See supra* paras. 25, 28.

[139] *See infra* paras. 36-40. The Companies assert that "the Commission will be unable to rely on the exception to APA review provided for abuses of discretion, given that the *Mathews* test—which the Commission failed to apply contrary to its own recent procedural order—provides a clear test for when an exercise of discretion is warranted and not warranted." PN/CN April 28, 2021 Reply at 35. As noted above, we have determined that the *Mathews* three-factor test supports the procedures we have adopted in this proceeding. *See supra* paras. 26-29.

[140] PN/CN April 28, 2021 Reply at 36.

[141] *Id.* at 42.

narrative."[142] The Companies contend that "[i]n this case, the Commission is acting as the investigator, prosecutor and finder of fact."[143]

32. We are unpersuaded by these arguments. We note that even under the subpart B hearing rules that the Companies would have the Commission apply, a hearing may be presided over by "an administrative law judge," "one or more commissioners," or "the Commission" itself.[144] Moreover, as we previously found in the *China Unicom Americas Order on Revocation* and the *China Telecom Americas Order on Revocation and Termination*, if the Commission were to delegate initial responsibility to an administrative law judge, the resulting decision could be appealed to the full Commission—which would be required to review the record independently and would not owe any deference to the administrative law judge's determinations.[145] As such, we are not persuaded by these contentions because the Companies have not adequately explained why the extra step of appointing an administrative law judge to preside prior to the Commission's independent review, rather than simply proceeding directly before the Commission, is necessary for or would enhance the ability of the Commission, which will be the ultimate arbiter, to decide any matter here. Importantly, at no point in this proceeding have the Companies been denied an opportunity to introduce evidence or arguments, and the Commission's decision here is based on the entire record. Moreover, with regard to the need for a neutral adjudicator or objective third party, the Companies fail to persuasively argue why the Commission or any individual Commissioner would not be able to serve as a neutral or objective decisionmaker in this case—and it has never moved for the recusal of any Commissioner. Absent any particularized and compelling reason why the Commission or any individual Commissioner would not be able to serve as a neutral decisionmaker in this matter, we find this contention unpersuasive. Finally, our decision to revoke the Companies' domestic section 214 authority and revoke and terminate their international section 214 authorizations is not a predetermined outcome but is based on the substantial record evidence developed in this matter.

c. Commission Did Not Impermissibly Avoid an Evidentiary Hearing as No Material Facts are in Dispute

33. Based on the record as a whole, we find that there are no substantial and material questions of fact in this matter warranting an adjudicatory hearing before an administrative law judge or other presiding officer. The record available to the Commission when it issued the *Institution Order* supported such a preliminary view,[146] and the current record developed since then has not persuaded us otherwise. The Companies contend that in this case, the Commission "has not asserted any material violation of the Commission's rules to precipitate the present proceeding" and instead "relies on sudden concerns about national security, new in the 12 years since Pacific Networks acquired ComNet and,

[142] *Id.* (citing, for example, Reply Comments of China Telecom (Americas) Corporation to Order Instituting Proceedings, GN Docket No. 20-109 (filed Mar. 1, 2021) at 2-3)).

[143] *Id*. The Companies add that this is unlike cases "[w]here relevant facts are readily apparent—a licensee has gone out of business, for example—[and] this kind of inquisitorial process is allowed for the sake of administrative expediency. But where there are as many facts in dispute as there are in this case, it should be a given that the facts will be reviewed by a neutral fact finder that has not interpreted every fact against the Companies." *Id.* at 42-43.

[144] 47 CFR § 1.241(a); *cf*. 5 U.S.C. § 556(b) (stating that a formal adjudication under the APA may be presided over by an administrative law judge, one or more members of the agency, or the "the agency" itself).

[145] *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 36 (citing *Kay v. FCC*, 396 F.3d 1184, 1189 (D.C. Cir. 2005) (explaining how "an agency reviewing an [administrative law judge] decision is not in a position analogous to a court of appeals reviewing a case tried to a district court")); *China Telecom Americas Order on Revocation and Termination* at *11, para. 29 (same).

[146] *See Institution Order*, 36 FCC Rcd at 6380, para. 19.

allegedly, utterly unable to be mitigated."[147] Significantly, the Companies assert that "the Commission's case, to the extent it is not based on unwarranted inferences, is based on material facts in dispute."[148]

34. Additionally, the Companies assert that the following facts are "clearly material to a revocation decision that are in dispute, and require adjudication by a neutral finder of fact,"[149] including: (1) whether the Companies are subject to the exploitation, influence and control of the Chinese government[150] and, therefore, whether they "raise not just 'significant national security and law enforcement risks' but 'pose a clear and imminent threat to the security of the United States due to Pacific Networks' and ComNet's access to U.S. telecommunications infrastructure,'"[151] (2) whether they "have or . . . would violate the law of the United States or their own data privacy policies . . . as well as the laws of the United States, by misusing access to [personally identifiable information and CPNI]," (3) whether they "can be trusted to 'cooperate with the U.S. government' regarding CALEA interception requests and hold in confidence the fact that such requests have been received,"[152] (4) the applicability of Chinese laws to the Companies and their operations, and (5) whether there are additional mitigation measures that would address the national security risks posed by the Companies.[153] Additionally, the Companies note that "there are discrepancies among statements made by the Companies to the Senate Subcommittee leading to the PSI Report on one hand and statements to Team Telecom and the Commission on the other about the degree of control exercised over the Companies by indirect owners and the location of and access to databases . . . ."[154] The Companies also note that the record of the China Telecom (Americas) Corporation proceeding shows that the Internet Governance Project at the Georgia Institute of Technology commented and filed an *ex parte* statement raising questions as to "whether alleged misrouting by China Telecom amounted to malicious hijacking."[155] They also contend that "[s]ince the *Institution Order* asserts that the Companies could engage in the same behavior, the basis for whether this type of conduct amounts to a real or imagined security threat engaged in by other Chinese companies is a material fact in dispute."[156]

35. We disagree and, based on our review of the record, we find that the question of whether revocation is appropriate does not turn on disputed issues of fact or questions of credibility for which an evidentiary hearing is necessary.[157] Our decision here is supported by a preponderance of the evidence in the overall record, including but not limited to facts that are not reasonably disputed as well as the assessments of the Executive Branch agencies of the overall national security and law enforcement risks. The disputes identified by the Companies and as we indicated in the *Institution Order*, "do not turn on witnesses testifying to their personal knowledge or observations or on individual credibility

[147] PN/CN April 28, 2021 Reply at 30.

[148] *Id*. at 26.

[149] *Id*. at 37.

[150] *Id*.

[151] *Id*. at 38.

[152] *Id*. at 39 (citing *Institution Order*, 36 FCC Rcd at 6404, para. 51).

[153] *Id*. at 41.

[154] *Id*. at 40.

[155] *Id*. at 39 (citing Comments of the Internet Governance Project, Georgia Institute of Technology's School of Public Policy, GN Docket No. 20-109 (filed Dec. 17, 2020) (Internet Governance Project Comments, GN Docket No. 20-109); Ex Parte Comments of the Internet Governance Project, Georgia Institute of Technology's School of Public Policy, GN Docket No. 20-109 (filed Mar 8, 2021) (Internet Governance Project *Ex Parte* Comments, GN Docket No. 20-109)).

[156] *Id*.

[157] *See Institution Order*, 36 FCC Rcd at 6378, para. 14.

determinations, for example, but instead on facts that can be fully ascertained through written evidence and on national security and law enforcement concerns associated with Pacific Networks' and ComNet's ultimate ownership and control by the Chinese government."[158] Indeed, in the following sections, we analyze the material facts alleged by the Companies to be in dispute,[159] and find the totality of the record evidence more than sufficient upon which to base our decisions.[160] And, the Companies have offered no new evidence that would dispel the Commission's prior analysis in the *Institution Order*, as discussed in this Order. Finally, we find that the Commission is exercising its well-established discretion[161] to proceed without holding an evidentiary hearing, and we base our decision today on the overall assessment of the public interest.

d. Procedures are Consistent with the Commission's Rules, Past Practice, and Precedent

36. The procedures adopted and outlined in the *Institution Order* are consistent with the Commission's rules, past practice, and precedent and are sufficient to resolve the ultimate questions in most section 214 cases while providing carriers with due process. Specifically, we reject the Companies' assertion that Commission precedent makes clear that an evidentiary hearing is warranted in this case.[162] As explained in the *Institution Order* and in similar cases,[163] it is well-established that the Commission's authority to "conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to the ends of justice"[164] includes the authority "to select the personnel and procedures that are best suited to the issues raised in each case and that will achieve a full, fair, and efficient resolution of each hearing proceeding."[165] While the Commission has relied upon live formal hearings before an administrative law judge in certain spectrum licensing proceedings, it has used other procedures for different types of proceedings when appropriate. For example, the Commission has generally resolved issues on a written record and without an administrative law judge in section 204 tariff proceedings and section 208 complaint proceedings.[166] Even when section 309 of the Act applies, the Commission has at times found it appropriate to proceed on the written record, for example, when evaluating competing

[158] *Id*. at 6380, para. 19.

[159] *See supra* para. 34 for a general description of the material facts the Companies allege are in dispute.

[160] *See generally infra* Sections III.B., III.C., III.D.

[161] *See China Unicom Americas Order on Revocation*, FCC 22-9 at para. 43 (citing *NextEra Energy Resources, LLC v. FERC*, 898 F.3d 14, 26 (D.C. Cir. 2018); *Ill. Commerce Comm'n v. FERC*, 721 F.3d 764, 776 (7th Cir. 2013) ("FERC need not conduct an oral hearing if it can adequately resolve factual disputes on the basis of written submissions.")); *China Telecom Americas Order on Revocation and Termination* at *16, para. 43 (same).

[162] PN/CN April 28, 2021 Reply at 33.

[163] *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 38; *China Telecom Americas Order on Revocation and Termination* at *7, para. 20; *Institution Order*, 36 FCC Rcd at 6377-78, para. 14; *China Unicom Americas Institution Order*, 36 FCC Rcd at 6328-29, para. 16; *China Telecom Americas Institution Order*, 35 FCC Rcd at 15015, para. 16.

[164] 47 U.S.C. § 154(j); *see FCC v. Schreiber,* 381 U.S. 279, 290 (1965); *FCC v. Pottsville Broadcasting Co.*, 309 U.S. 134, 138 (1940) (holding that "the subordinate questions of procedure in ascertaining the public interest, when the Commission's licensing authority is invoked . . . [are] explicitly and by implication left to the Commission's own devising" by section 4(j) of the Act, "so long, of course, as it observes the basic requirements designed for the protection of private as well as public interest"); *see also Vermont Yankee Nuclear Power Corp. v. Natural Resources Defense Council, Inc.,* 435 U.S. 519, 524-25 (1978); *id.* at 543-44 (noting the "very basic tenet of administrative law that agencies should be free to fashion their own rules of procedure").

[165] *Administrative Hearings Order*, 35 FCC Rcd at 10731, para. 7.

[166] *Id.* at 10730, para. 3 (citing *July 1, 2018 Annual Access Charge Tariff Filings; South Dakota Network, LLC Tariff F.C.C. No.1*, Memorandum Opinion and Order, 34 FCC Rcd 1525 (2019); 47 CFR §§ 1.720-.736).

initial cellular applications and in license-renewal and transfer proceedings where the Commission has determined that there are no substantial issues of material fact or credibility issues.[167]

37. As we previously observed,[168] there is no statutory obligation that requires us to follow any specific procedures in the instant matter.[169] In the Companies' Response to the *Order to Show Cause*, they assert that "[t]he Commission consistently has ordered administrative hearings when considering whether to revoke Section 214 authorizations or to issue orders to cease and desist common carrier operations, relying on Sections 154(i), 214 and 321 of the Act and Section 1.91 of the Commission's rules,"[170] identifying several cases between 1997 and 2007 in which the Commission designated for hearing the revocation of section 214 authorizations.[171] The Companies contend that the Commission has only revoked section 214 authorizations without holding an evidentiary hearing "in cases where the respondent has failed to respond to notices from the Commission. In those limited instances, that [sic] companies had failed to respond to multiple inquiries from the Commission and had presumably gone out of business, making a hearing unnecessary."[172] The Companies add that "absent those unusual circumstances, and as explained in [the Companies' Response to the *Order to Show Cause*], the Commission designated [s]ection 214 authorizations for hearing and provided the respondent an opportunity to be heard."[173]

38. As we noted in the *Institution Order* and related proceedings, those cases reflect nothing more than the Commission's lawful exercise of its discretion to order a hearing in a particular dispute under section 214 of the Act.[174] Although the Companies attempt to distinguish those cases, they

[167] *Id.* at 10730, para. 4 (citing *Inquiry into the Use of the Bands 825-845 MHz and 870-890 MHz for Cellular Communications Systems*, Report and Order, 86 FCC 2d 469 (1981); *Birach Broad. Corp.*, Hearing Designation Order, 33 FCC Rcd 852 (2018); *Radioactive, LLC*, Hearing Designation Order, 32 FCC Rcd 6392 (2017)). *See also Applications of T-Mobile US, Inc. and Sprint Corp.*, Memorandum Opinion and Order, Declaratory Ruling, and Order of Proposed Modification, 34 FCC Rcd 10578, 10596, para. 42 (2019); *Gencom Inc. v. FCC*, 832 F.2d 171 (D.C. Cir. 1987).

[168] *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 39; *China Telecom Americas Order on Revocation and Termination* at *8, para. 21; *Institution Order*, 36 FCC Rcd at 6377-78, para. 14; *China Unicom Americas Institution Order*, 36 FCC Rcd at 6328-29, para. 16.

[169] Additionally, as discussed above, the basis for instituting these proceedings does not turn on any disputed facts that would benefit from being examined in a hearing before an administrative law judge. *See infra* paras. 33-35.

[170] PN/CN June 1, 2020 Response at 36.

[171] *Id*. at 36 n.71 (citing *CCN, Inc. Order to Show Cause*, 12 FCC Rcd at 8560-62, paras. 21-22, *CCN, Inc. Order*, 13 FCC Rcd at 13607, para. 13; *Publix Order*, 17 FCC Rcd at 11506-09, paras 44-45; *Business Options Order*, 18 FCC Rcd at 6893-94, paras 33-35, 38; *NOS Communications Order*, 18 FCC Rcd at 6964-65, paras. 25-26, 29; and *Kintzel Order*, 22 FCC Rcd at 17205-07, paras. 24-25). Significantly, none of those matters were ultimately resolved through a hearing under the subpart B rules.

[172] PN/CN April 28, 2021 Reply at 33 (citing, for example, *Wypoint Telecom, Inc. Termination of International Section 214 Authorization*, Order, 30 FCC Rcd 13431, 13432-33, para. 4 (IB-PD 2015); *LDC Telecommunications, Inc.*, Revocation Order, 31 FCC Rcd 11661, 11662, para. 5 (EB-TCD, IB-TAD & WBC-CPD 2016) (revoking domestic and international Section 214 authorizations for failure to pay regulatory fees after carrier failed to respond to order to show cause); *WX Communications Ltd. Termination of International Section 214 Authorization*, Order, 34 FCC Rcd 1028, 1029-30, para. 5 (IB-TAD 2019)).

[173] *Id*. (citing PN/CN June 1, 2020 Response at 36-37). The Companies note that "[t]he hearing was not a mere formality in those circumstances, but rather provided the respondent an opportunity to raise specific evidentiary questions and to be heard by an unbiased arbitrator of fact." *Id.* at 33-34.

[174] *See Institution Order*, 36 FCC Rcd at 6379, para. 16 (citing *Application of Oklahoma W. Tel. Co.*, Order, 10 FCC Rcd 2243, 2243-44, para. 6 (1995) (*Oklahoma W. Tel. Co. Order*) (stating that "the Commission has the discretion to designate for evidentiary hearing issues raised in the context of a [s]ection 214 application")); *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 39 (same); *China Telecom Americas Order on Revocation and*

(continued….)

demonstrate that the Commission has not applied subpart B hearing rules to all section 214 revocation proceedings. Thus, contrary to the Companies' view, the Commission has never had an established practice of requiring subpart B hearings for all section 214 revocations.[175] Rather, we find that the handful of cases on which the Companies seek to selectively rely simply reflect the tailoring of procedures according to the circumstances of each case, and in the exercise of the Commission's broad procedural discretion under section 4(j) of the Act.[176]

39. Because we disagree with the Companies' premise that the Commission has changed its position, we disagree with their claim that the Commission has not provided "a reasoned justification for changing positions on existing policies."[177] The Companies state that the Commission "cites to 'relevant national security issues' and [the] 'public interest' as warranting a prompt response,"[178] but observe that "this particular process has lasted over a year and could have been well down the road towards a full hearing by now" and that "[t]hose same complex, important concerns are all the more reason to ensure a thorough investigation and opportunity to be heard before an Administrative Law Judge."[179] As we stated in the *Institution Order* and in related proceedings, even if prior cases were thought to represent a past policy of applying subpart B to all section 214 revocations, we no longer believe that such a policy is appropriate, particularly not in cases where the pleadings addressing the relevant national security issues do not identify any need for additional procedures and the public interest warrants prompt response to

(Continued from previous page)
Termination at *8, para. 21 (same); *China Unicom Americas Institution Order*, 36 FCC Rcd at 6330, para. 18 (same).

[175] *See China Unicom Americas Order on Revocation*, FCC 22-9 at para. 39; *China Telecom Americas Order on Revocation and Termination* at *8, para. 21; *Institution Order*, 36 FCC Rcd at 6379, para. 16; *China Unicom Americas Institution Order*, 36 FCC Rcd at 6330, para. 18.

[176] In contrast with the questions before us, which we can resolve based on the existing record without an evidentiary hearing, in the cases cited by the Companies, the Commission exercised its discretion to refer the matter to an administrative law judge to ascertain underlying facts regarding the nature of the conduct at issue and whether it violated Commission rules or the Communications Act, in light of apparent concealment of these facts from Commission staff and misrepresentations to consumers. In the *CCN, Inc. Order to Show Cause*, the Commission had received numerous consumer complaints about allegedly forged or falsified information resulting in unauthorized changes in service (i.e., slamming), and it appeared that the authorization holder was deliberately frustrating staff's efforts to investigate the complaints. *CCN, Inc. Order to Show Cause,* 12 FCC Rcd 8547. The *Business Options Order* likewise concerned alleged slamming violations and concerns about misrepresentation and lack of candor before the Commission. *Business Options Order,* 18 FCC Rcd 6881. The *Kintzel Order* involved allegations of slamming and cramming as well as failure to make required contributions to the Universal Service and Telecommunications Relay Services (TRS) funds, and noncompliance with a consent decree intended to address prior violations; among other things, the administrative law judge was directed to determine whether specified forfeitures were warranted for enumerated violations in the event the authorizations were not revoked. *Kintzel Order*, 22 FCC Rcd 17197. In the *Publix Order*, the Commission pointed to a number of factual questions to be resolved based on concerns that Publix had "unlawfully obtained over six million dollars in payments from the TRS Fund by means of a scheme to create the appearance that they were operating a legitimate telecommunications relay service," had misrepresented facts to the Commission, and had violated numerous Commission rules. *Publix Order,* 17 FCC Rcd at 11487-88. The *NOS Communications Order* involved willful and repeated apparent violations of the Commission's rules based on a "misleading and continuous telemarketing campaign." *NOS Communications Order*, 18 FCC Rcd at 6953.

[177] PN/CN April 28, 2021 Reply at 34 (citing *Encino Motorcars, LLC v. Navarro,* 136 S. Ct. 2117, 2125-26 (2016) ("Agencies are free to change their existing policies as long as they provide a reasoned explanation for the change . . . . [T]he agency must at least 'display awareness that it is changing position' and 'show that there are good reasons for the new policy.'") (*quoting FCC v. Fox Television Stations, Inc.,* 556 U.S. 502, 515 (2009))).

[178] PN/CN April 28, 2021 Reply at 34 (citing *Institution Order*, 36 FCC Rcd at 6379-80, para. 17).

[179] *Id.*

legitimate concerns raised by the Executive Branch without conducting an evidentiary hearing,[180] after full and thorough consideration of the issues presented and the totality of the record evidence.[181]

40. More importantly, the Commission has never applied its subpart B hearing rules to every adjudication.[182] Section 1.91 of the Commission's rules applies subpart B hearing rules to revocations of "station license[s]" or "construction permit[s]"—terms that refer to spectrum licenses issued under Title III of the Act—but, in contrast to an adjacent section of those rules, does not extend to section 214 authorizations.[183] This distinction reflects one in the Act itself, which specifies a procedure for revoking Title III authorizations in section 312,[184] but does not specify any such required procedure for revoking Title II authorizations. Thus, in the recent proceeding updating the Commission's subpart B hearing rules, the Commission noted that "the hearing requirements applicable to Title III radio applications do not apply to Title II section 214 applications."[185]

(i) An Adjudication is Appropriate Here

41. We again reject the Companies' argument that the Commission's actions in this case are more appropriately considered through a rulemaking process.[186] As part of their contention that the

[180] *See supra* paras. 26-29 (discussing *Mathews* factors weighing in favor of relying on written procedures in this case).

[181] *Institution Order*, 36 FCC Rcd at 6379-80, para. 17; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 40; *China Telecom Americas Order on Revocation and Termination* at *8, para. 21; *China Unicom Americas Institution Order*, 36 FCC Rcd at 6330, para. 19; *see Fox Television*, 556 U.S. at 515; *see, e.g.*, *CBS Corp. v. FCC*, 785 F.3d 699, 708 (D.C. Cir. 2015).

[182] In fact, section 1.201 of those rules provides that subpart B applies only to cases that "have been designated for hearing." 47 CFR § 1.201. An explanatory note makes clear that the new procedures for written hearings are a subset of such cases. *Id.* Note 1. *See Procedural Streamlining of Administrative Hearings*, Notice of Proposed Rulemaking, 34 FCC Rcd 8341, 8343, para. 4 & n.16 (2019) (*Administrative Hearings NPRM*). In the *Administrative Hearings Order*, the Commission adopted and incorporated by reference all the rules described in the *Administrative Hearings NPRM* with minor modification, and adopted and incorporated by reference and further elaborated on the legal arguments and justification presented in the *Administrative Hearings NPRM* in support of the rules adopted in the Order. *Administrative Hearings Order*, 35 FCC Rcd at 10731, para. 8.

[183] 47 CFR § 1.91; *compare id.* § 1.89 (applying to "any person who holds a license, permit[,] *or other authorization*" (emphasis added)). The Act defines "station license" to mean "that instrument of authorization required by this chapter or the rules and regulations of the Commission made pursuant to this chapter, for the use or operation of apparatus for transmission of energy, or communications, or signals by radio, by whatever name the instrument may be designated by the Commission." 47 U.S.C. § 153(49); *see also id*. §§ 307-310, 319. A "construction permit" is "that instrument of authorization required by this chapter or the rules and regulations of the Commission made pursuant to this chapter for the construction of a station, or the installation of apparatus, for the transmission of energy, or communications, or signals by radio, by whatever name the instrument may be designated by the Commission." *Id.* § 153(13). By contrast, telecommunications carriers obtain a "certificate" or an "authorization" under section 214, not a radio "station license or construction permit." *See* 47 U.S.C. § 214(a) (stating that a carrier must obtain from the Commission "a certificate that the present or future public convenience and necessity require or will require . . . "); 47 CFR §§ 63.01 ("Authority for all domestic common carriers."), 63.21 ("Conditions applicable to all international Section 214 authorizations.").

[184] 47 U.S.C. § 312(c).

[185] *Administrative Hearings NPRM*, 34 FCC Rcd at 8343, para. 4 & n.16 (internal quotations and alteration omitted); *Oklahoma W. Tel. Co. Order*, 10 FCC Rcd at 2243-44, para. 6 (finding no substantial public interest questions existed to justify hearing on section 214 application) (citing *ITT World Commc'ns v. FCC*, 595 F.2d 897, 900-01 (2d Cir. 1979)). *See China Unicom Americas Order on Revocation*, FCC 22-9 at para. 41; *China Telecom Americas Order on Revocation and Termination* at *8, para. 22; *Institution Order*, 36 FCC Rcd at 6379, para. 15; *China Unicom Americas Institution Order*, 36 FCC Rcd at 6330, para. 17.

[186] PN/CN April 28, 2021 Reply at 28.

process we adopted is fundamentally unfair in light of Commission precedent, the Companies reiterate their argument from their Response to the *Order to Show Cause* that "the questions at issue in this proceeding are serious and extensive enough to warrant a rulemaking proceeding to ensure that the new procedural and substantive requirements applicable to all [s]ection 214 holders could be comprehensively reviewed to avoid inconsistent enforcement and protect against violations of due process."[187] The Companies argue that "the Commission waved these questions away, simply reiterating its 'very broad discretion' to proceed by adjudication or rulemaking" and that "the issues raised here are best resolved through "party-specific procedures."[188] The Companies have provided no additional evidence or persuasive argument to dispel the well-established principle that, "in interpreting and administering its statutory obligations under the Act, the Commission has very broad discretion to decide whether to proceed by adjudication or rulemaking,"[189] nor our prior determination that the issues raised here best lend themselves to resolution through the party-specific procedures adopted in this proceeding.[190] Again, the Companies had ample opportunity to contest the allegations raised in this matter with their own evidence.

(ii) Commission Accorded Appropriate Deference to the Executive Branch Agencies

42. Contrary to the Companies' assertions, the Commission properly consulted and accorded the appropriate deference to the views of the relevant Executive Branch agencies in this matter. The Companies observe, among other things, that the Executive Branch agencies' November 16, 2020 Letter (1) did not offer a recommendation by the Committee that the Commission take any particular action with respect to the Companies "[g]iven the nature of the Commission's request for views on discreet factual questions, and the limited time allotted for response,"[191] (2) does not "address any of the Companies' arguments [but] reiterates arguments raised against China Telecom and China Unicom regarding the 'inherent national security risks attach[ed] to telecommunications companies owned or controlled by the Chinese government' and the asserted coercive effect of Chinese law,'"[192] (3) provided a general analysis, not specific to the Companies, that could be applied to any Chinese state-owned company,[193] and (4)

[187] *Id.* (citing PN/CN June 1, 2020 Response at paras. 27-30). The Companies also argue that "[s]eparately, while the Commission is admittedly given broad latitude to decide between proceeding by rulemaking and proceeding by adjudication, the Commission's bare minimum justification for continuing this process without a comprehensive rulemaking, despite the extensive unanswered questions raised by this extraordinary process, is reasonably viewed as crossing outside the boundary of the agency's discretion." *Id.* at 35-36.

[188] *Id.* at 28 (citing *Institution Order*, 36 FCC Rcd at 6381-82, para. 21).

[189] *See, e.g.*, *Neustar, Inc. v. FCC*, 857 F.3d 886, 894 (D.C. Cir. 2017) (internal quotation marks and citations omitted); *Chisholm v. FCC*, 538 F.2d 349, 365 (D.C. Cir. 1976) (reiterating that "the choice whether to proceed by rulemaking or adjudication is primarily one for the agency regardless of whether the decision may affect agency policy and have general prospective application") (citing *N.L.R.B. v. Bell Aerospace Co.*, 416 U.S. 267, 291-95 (1974); *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947) (stating that "the choice made between proceeding by general rule or by individual, *ad hoc* litigation is one that lies primarily in the informed discretion of the administrative agency"); *SBC Communications, Inc. v. FCC*, 138 F.3d 410, 421 (D.C. Cir. 1998) (stating that "[i]nherent in an agency's ability to choose adjudication rather than rulemaking . . . is the option to make policy choices in small steps, and only as a case obliges it to") (citation omitted).

[190] *Institution Order*, 36 FCC Rcd at 6381-82, para. 21.

[191] PN/CN April 28, 2021 Reply at 5 (citing Executive Branch Nov. 16, 2020 Letter at 1).

[192] *Id.* (citing Executive Branch Nov. 16, 2020 Letter at 2).

[193] *Id.* at 6. The Companies state that the Executive Branch agencies' letter "does not specifically analyze the Retail Calling Card, Wholesale IDD or MPLS VPN services provided by the Companies, instead simply concluding that the very interconnection of the Companies' networks provides 'an opportunity for exploitation.'" *Id.* (citing Executive Branch Nov. 16, 2020 Letter at 8, 10). The Companies also note that the general language in the letter is "substantially a copy of language provided in the Executive Branch agencies' separate, much longer, response regarding China Unicom [Americas]." *Id*. (citing Executive Branch Nov. 16, 2020 Letter).

stated that it was not a "recommendation" and that DOJ and DHS "have not identified acts of non-compliance under the minimal conditions placed on the Companies' Section 214 authorizations."[194]

43. The Executive Branch agencies specifically state that their response is not offered as a recommendation by the Committee pursuant to Section 6 of Executive Order 13913. Instead, they have offered their views pursuant to their discretion to communicate information to the Commission under the Executive Order.[195] The Commission does not require a formal "recommendation" from the Committee but can consider the information provided by the relevant Executive Branch agencies in making its public interest determination.[196] Additionally, the Executive Branch agencies have advised that "(1) the [2009] LOA is no longer adequate to protect [from] the risk posed by the Companies to law enforcement and national security interests; and (2) amending the LOA to add new mitigation measures is inadequate to protect law enforcement and national security interests because the Monitoring Agencies lack confidence that the Companies will comply with additional restrictions if those obligations conflict with the [Chinese government's] updated legal requirements, which the entities in the Companies' corporate chain must follow."[197]

B. Revocation of Section 214 Authority

44. Based on our public interest analysis under section 214 of the Act and the totality of the extensive record evidence, we find that the present and future public interest, convenience, and necessity is no longer served by the Companies' retention of their section 214 authority, and we revoke their domestic and international section 214 authority.[198] *First*, the record shows that Pacific Networks and ComNet are U.S. subsidiaries of a Chinese state-owned entity, and therefore they are subject to exploitation, influence, and control by the Chinese government and are highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight. *Second*, given the changed national security environment with respect to China since the Commission authorized the Companies to provide telecommunications services in the United States, we find that the Companies' ownership and control by the Chinese government raise significant national security and law enforcement risks by providing opportunities for the Companies, their parent entities and affiliates, and the Chinese government to access, monitor, store, and in some cases disrupt and/or misroute U.S. communications, which in turn allow them to engage in espionage and other harmful activities against the United States. *Third*, independent of these concerns, the Companies' conduct and representations to the Commission and Congress demonstrate a lack of trustworthiness and reliability that erodes the baseline level of trust that the Commission and other U.S. government agencies require of telecommunications carriers given the critical nature of the provision of telecommunications service in

[194] *Id.* at 6 (citing Executive Branch Nov. 16, 2020 Letter at 10).

[195] Executive Branch Nov. 16, 2020 Letter at 1 (citing, for example, Executive Order 13913, §§ 10(h)(ii), 12(a)(i)).

[196] The Commission has a longstanding policy of according deference to the Executive Branch agencies' expertise in identifying risks to national security and law enforcement interests. *See supra* para. 5; *see also China Mobile USA Order*, 34 FCC Rcd at 3362, para. 2; *Huawei Designation Order*, 35 FCC Rcd at 14448, para. 34 & n.117; *China Telecom Americas Institution Order*, 35 FCC Rcd at 15017, para. 21; *China Telecom Americas Order on Revocation and Termination* at *2, para. 5; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 5. The Commission ultimately makes an independent decision in light of the information in the record, including any information provided by the applicant, authorization holder, or licensee in response to any filings by the Executive Branch agencies. *Foreign Participation Order*, 12 FCC Rcd at 23921, para. 66 ("We emphasize that the Commission will make an independent decision on applications to be considered and will evaluate concerns raised by the Executive Branch agencies in light of all the issues raised (and comments in response) in the context of a particular application.").

[197] Executive Branch June 4, 2021 Reply at 2 (citing Executive Branch Nov. 16, 2020 Letter at 6, 10). *See infra* Section III.D.

[198] *See generally Institution Order.*

the United States. We find that these risks cannot be addressed through further mitigation with the Executive Branch agencies.

1. The Companies are Majority-Owned and Controlled by the Chinese Government

45. The record evidence overwhelmingly shows that the Companies are not separate and independent from their parent entities and supports the Executive Branch agencies' assessment that the Companies are subject to exploitation, influence, and control by the Chinese government.[199] The record is clear that Pacific Networks and ComNet are majority-owned and controlled by the Chinese government through CITIC Group Corporation, a Chinese state-owned limited liability company.[200] We agree with the Executive Branch agencies' assessment that "[t]he Chinese government's majority ownership and control of the Companies through [CITIC Group Corporation], combined with Chinese intelligence and cybersecurity laws, raise significant concerns that the Companies will be forced to comply with Chinese government requests, including requests for communications intercepts, without the ability to challenge such requests."[201] These laws include the National Intelligence Law of the People's Republic of China, effective June 28, 2017 (2017 National Intelligence Law),[202] the Cybersecurity Law of the People's Republic of China, effective June 1, 2017 (2017 Cybersecurity Law),[203] and the 2019 Cryptography

[199] *See* Executive Branch Nov. 16, 2020 Letter at 2-12.

[200] *See supra* para. 7 & notes 26, 27; PN/CN June 1, 2020 Response at 10 ("At each link in the ownership chain, except for two, the aggregate ultimate ownership held indirectly by CITIC Group Corporation is 100%. The two links in the ownership chain which represent less than 100% ownership by CITIC Group are: (1) the ownership by CITIC Polaris Limited and CITIC Glory Limited, each of which is a direct wholly-owned subsidiary of CITIC Group Corporation, of an aggregate of 58.13% of the equity of CITIC Limited, a publicly-traded company the stock of which is listed on the Hong Kong Stock Exchange, and (2) the ownership by Richtone Enterprises Inc., Ease Action Investments Corp., Perfect New Holdings Limited and Silver Log Holdings Ltd., each of which is an indirect controlled subsidiary of CITIC Group Corporation, of an aggregate of 58.12% of the equity of CITIC Telecom International Holdings Limited ('CITIC Tel'), a publicly-traded company the stock of which is listed on the Hong Kong Stock Exchange."); *id.* at 33-34 (describing the organizational chart attached as Exhibit A and stating, "each of those links represents over 50% ownership and therefore control" and "the links would be treated as constituting control under the Commission's rules"); *id.*, Exh. A (Pacific Networks & ComNet Organization Chart as of May 28, 2020); *id.* at ii ("an investment company owned by the People's Republic of China holds an indirect ownership interest in the Companies in excess of 50%"); *id.* at 26 ("the Chinese government's majority ownership in the Companies"); PN/CN April 28, 2021 Reply at ii ("an investment company owned by the People's Republic of China holds an indirect ownership interest in the Companies in excess of 50%"); *id.* at 43 ("The Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation"); 2012 Pacific Networks Pro Forma TC Notification, Attach. 1 at 1-2, Exhs. A, B (describing "CITIC Group Corporation" as "a state-owned limited liability company"); 2012 ComNet Pro Forma TC Notification, Attach. 1 at 1-2, Exhs. A, B (describing "CITIC Group Corporation" as "a state-owned limited liability company"); *Institution Order*, 36 FCC Rcd at 6372-73, para. 5; *Order to Show Cause*, 35 FCC Rcd at 3734-35, para. 4; Executive Branch Nov. 16, 2020 Letter at 2, 6, 11-12.

[201] Executive Branch Nov. 16, 2020 Letter at 6; *Institution Order*, 36 FCC Rcd at 6383-84, para. 24.

[202] Executive Branch Nov. 16, 2020 Letter at 6-8; *Institution Order*, 36 FCC Rcd at 6384, para. 24; China Law Translate, National Intelligence Law of the P.R.C. (2017) (Passed on June 27, 2017 and effective June 28, 2017), https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/ (last visited Mar. 18, 2022); *see* The National People's Congress of the People's Republic of China, *National Intelligence Law of the People's Republic of China*, http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/27/content_2024529 htm (last visited Mar. 8, 2022).

[203] Executive Branch Nov. 16, 2020 Letter at 6-8; *Institution Order*, 36 FCC Rcd at 6384, para. 24; Translation: Cybersecurity Law of the People's Republic of China (Passed November 6, 2016 and effective June 1, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (English translation as of June 29, 2018); *see* The National People's Congress of the People's Republic of

(continued….)

Law.[204] Indeed, a former U.S. National Security Advisor cautioned about "the integrated nature of the Chinese Communist Party's military and economic strategies," stating that the Chinese Communist Party "is obsessed with control—both internally and externally," and that under Article 7 of China's National Intelligence Law, "all Chinese companies must collaborate in gathering intelligence."[205] Further, the PSI Report found, among other things, that "Chinese state-owned companies are subject to an added layer of state influence in that they must comply with strict national security, intelligence, and cyber security laws regardless of where they operate."[206] Based on the record, and consistent with the Commission's findings in other related proceedings, we find the arguments of the Executive Branch agencies persuasive.

46. *CITIC Tel Exerts Significant Influence and Control Over the Companies' Business and Information Security Operations.* We find that the Companies' claims about their "factual and legal independence from Chinese government influence"[207] are contradicted by the record and the Commission's findings in other related proceedings.[208] The Companies claim that they are "small, independently-operated, U.S. domiciled companies that are not wholly-owned by the Chinese government"[209] and that "[i]n terms of day-to-day management, [they] conduct their operations independently."[210] The Companies contend that the "[e]ntities upstream of [Pacific Choice International Limited] are not involved in the daily business or operations of Pacific Networks or ComNet."[211] The Companies add, "[e]xecutives of their parent corporations do not participate in the daily operations of

(Continued from previous page)
China, *Cybersecurity Law of the People's Republic of China*, http://www.xinhuanet.com//politics/2016-11/07/c_1119867015.htm (last visited Mar. 8, 2022).

[204] Executive Branch Nov. 16, 2020 Letter at 6-8 (citing Dangerous Partners: Big Tech and Beijing: Hearing Before the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, 116th Congress (Mar. 4, 2020) (Statement of Deputy Assistant Attorney General Adam S. Hickey, National Security Division, U.S. Department of Justice)); *Institution Order*, 36 FCC Rcd at 6384, para. 24; China Law Translate, Cryptography Law of the P.R.C. (2019), https://www.chinalawtranslate.com/en/cryptography-law/ (last visited Mar. 17, 2022); *see* The National People's Congress of the People's Republic of China, Cryptography Law of the People's Republic of China (Passed Oct. 26, 2019, Effective Jan. 1, 2020), http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml (last visited Mar. 8, 2022). The Cryptography Law was adopted on October 26, 2019 and became effective on January 1, 2020. *See* Lawinfochina, Cryptography Law of the People's Republic of China, https://www.lawinfochina.com/display.aspx?id=31389&lib=law&SearchKeyword=cryptography%20law&SearchCKeyword= (last visited Mar. 18, 2022) (reflecting "Date issued" as October 26, 2019 and "Effective date" as January 1, 2020). We refer to the Cryptography Law herein as the "2019 Cryptography Law" for consistency with this usage by the Executive Branch agencies, but we note that DHS has publicly referred to the same law as the "The [People's Republic of China] Cryptography Law of 2020." *See* Executive Branch Nov. 16, 2020 Letter at 6 (citing Statement of Deputy Assistant Attorney General Adam S. Hickey, National Security Division, U.S. Department of Justice); *see infra* note 389.

[205] H.R. McMaster, *What China Wants*, The Atlantic, May 2020, at 70, 71, 72-73 (*What China Wants*), *available at* https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/.

[206] PSI Report at 9.

[207] PN/CN June 1, 2020 Response at 27.

[208] *See China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17; *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, 11442, paras. 46, 49; *Huawei Designation Order*, 35 FCC Rcd at 14440-42, paras. 16-17, 20.

[209] PN/CN June 1, 2020 Response at 26.

[210] *Id*. at 11.

[211] *Id*. The Companies "certify under penalty of perjury" that "Pacific Networks and ComNet are wholly-owned subsidiaries of Pacific Choice International Limited and that company's parent corporation [is] CITIC Telecom International Holdings Limited [(CITIC Tel)]." *Id.*, Declaration of Li Ying (Linda) Peng.

ComNet or Pacific Networks."[212] In their response to the *Order to Show Cause*, the Companies state that "[t]he financial positions of Pacific Networks and ComNet are routinely reviewed by CITIC Tel, but they do not assess or require changes in the Companies' technical or network operations."[213] In the *Institution Order*, we stated, among the Companies' various omissions, that the Companies reported to the Senate Subcommittee—but not to the Commission in their response to the *Order to Show Cause*—that "'[CITIC Tel] also guides ComNet on its information security policies.'"[214] In their response to the *Institution Order*, however, the Companies state that they "should have clarified that while the Companies' indirect owners may not require that specific technical decisions be made on a day-to-day basis, the Companies *observe* guidance from CITIC Tel regarding network security."[215] The Companies insist, nonetheless, on "the limited nature of involvement by indirect owners and their executives."[216]

47. Contrary to the Companies' arguments, the record evidence demonstrates that the Companies are not independent and that their parent entities have the ability to exercise significant and substantial influence and control over the Companies. The Companies' relationship with their indirect parent entity, CITIC Tel,[217] is neither "limited" nor confined to CITIC Tel "routinely review[ing] . . . financial positions."[218] In fact, the Companies admit in their response to the *Institution Order* that the "routine" reviews actually involve reporting monthly and annual financial updates to CITIC Tel, and that CITIC Tel also performs periodic audits of the Companies' IT governance, human resources process, risk management, and other audits, and may require the Companies to take certain remediation actions.[219] Specifically, the Companies state that, "[o]n an annual basis, the Companies submit to CITIC Tel their Annual Operating Plan ('AOP') detailing their budgets, revenue and operating expenditures for the upcoming three years, together with the forecasted actual numbers of the current year"[220] and "[m]onthly financial information is reported to CITIC Tel for group consolidation purposes and the Companies' local management team will explain any material variation from the AOP."[221] The Companies further state that, "[p]eriodically, CITIC Tel's internal and external auditors will perform IT governance audits of the Companies, as part of larger audits of the operations of CITIC Tel and its subsidiaries."[222] According to

[212] *Id*., Declaration of Li Ying (Linda) Peng.

[213] *Id*. at 11.

[214] *See Institution Order*, 36 FCC Rcd at 6385, para. 26 (quoting PSI Report at 95-96); PSI Report at 95-96 (citing Briefing with ComNet (Apr. 13, 2020)).

[215] PN/CN April 28, 2021 Reply at 69-70 (emphasis added).

[216] *Id*. at 65-66.

[217] Based on the record, CITIC Tel holds a direct 100% ownership interest in Pacific Choice International Limited, which in turn holds a direct 100% ownership interest in Pacific Networks. PN/CN June 1, 2020 Response, Exh. A (Pacific Networks and ComNet Organization Chart as of May 28, 2020); *id.* at 10 (stating, "[t]he current ownership structure of Pacific Networks and ComNet, direct and indirect, and the place of organization of each entity in the ownership structure is set forth on the organizational chart attached hereto as Exhibit A"); PN/CN April 28, 2021 Reply at 66 (referring to CITIC Tel as "the parent company"). Based on the record, CITIC Tel is "a publicly-traded company" that is incorporated and listed in Hong Kong. *See* PN/CN June 1, 2020 Response at 10; *id.*, Exh. A.

[218] PN/CN April 28, 2021 Reply at 65-66; PN/CN June 1, 2020 Response at 25; *see id.* at 11.

[219] PN/CN April 28, 2021 Reply at 43-44.

[220] *Id*. at 43. According to the Companies, "[t]he AOP is prepared by each Company to show material variances between the budgeted and forecasted actual, which are then discussed with CITIC Tel." *Id.*

[221] *Id*. The Companies state that, "[a]s part of the oversight of the Companies' financial positions, CITIC Tel has provided guidance to the Companies from time to time regarding changes in accounting standards or specific accounting issues as they may arise." *Id.*

[222] *Id*. at 44. Additionally, the Companies state that, "[r]elated to financial matters, CITIC Tel's internal and external auditors also perform periodic audits on the Companies' treasury processes, cash management process,

(continued….)

the Companies, "[a]ny findings, together with remediation actions, are discussed and agreed with the Companies and reported to the executive directors of CITIC Tel."[223] We find that these admissions undermine the assertion that the Companies are independent from CITIC Tel, and further demonstrate how integrated the Companies' business and information security operations are with those of CITIC Tel.

48. *The Companies' Corporate Leadership is Closely Associated with the Corporate Leadership of the Companies' Parent Entities.* As an initial matter, we find that the Companies failed to fully respond to the directive to include "an identification of all officers, directors, and other senior management of all entities that hold a ten percent or greater *direct or indirect* ownership interest in and/or control Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government."[224] The Companies failed to provide responsive information for most of the entities in their vertical chain of ownership that hold 10% or greater ownership interest, which they admit in their response to the *Order to Show Cause* "consists of numerous separate entities."[225] Although the Companies identify three entities—CITIC Tel, CITIC Limited, and CITIC Group Corporation—in response to this directive in the *Institution Order*,[226] the Companies merely direct the Commission to those entities' public websites without providing with specificity the information requested by the Commission concerning the identity of the individuals comprising the corporate leadership of the Companies' parent entities.[227] This reinforces our view, as set forth in the *Institution Order*, that the Companies' failure to fully respond to the *Order to Show Cause* raises troubling questions about their transparency and reliability.[228]

(Continued from previous page)
fixed assets management process, human resources process, inventory management process, credit control, financial system, risk management, and financial reporting." *Id.*

[223] *Id*.

[224] *Institution Order*, 36 FCC Rcd at 6415, Appx. A (emphasis added); *see Order to Show Cause*, 35 FCC Rcd at 3737, para. 9 ("Pacific Networks and ComNet shall include in their response the following information . . . an identification of all officers, directors, and other senior management officials of entities that hold [10%] or greater ownership interest in Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government."). As discussed in Section III.B.3, the Companies' failure to fully respond to the *Order to Show Cause* and the *Institution Order* raises serious concerns about their transparency and reliability. *See infra* Section III.B.3.

[225] PN CN June 1, 2020 Response at 11-12; PN/CN April 28, 2021 Reply at 45-46 (stating, "[t]he Companies refer the Commission to the information provided in the [Order to Show Cause] Response" and claiming, "[f]urther, information about the officers, directors and other senior management of the following entities that hold a [10%] or greater ownership interest in and/or control Pacific Networks and ComNet is provided . . . ."); *Institution Order*, 36 FCC Rcd at 6391, para. 34 (stating, "Pacific Networks and ComNet also failed to fully respond to the directive in the *Order to Show Cause* to include 'an identification of all officers, directors, and other senior management officials of entities that hold [10%] or greater ownership interest in Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government.' Pacific Networks and ComNet submitted such information for only one entity, Pacific Choice International Limited, even though they state that 'the upstream ownership structure of Pacific Networks and ComNet consists of numerous separate entities.'").

[226] *See* PN/CN April 28, 2021 Reply at 45-46.

[227] *See id*.; *see also infra* Section III.B.3.

[228] *Institution Order*, 36 FCC Rcd at 6408, para. 58 & n.277 (stating that instead of providing the requisite information for other entities that hold 10% or greater ownership interest in the Companies, "Pacific Networks and ComNet direct the Commission to look at the public record"); *see Order to Show Cause*, 35 FCC Rcd at 3737, para. 9; *see infra* Section III.B.3.

49. Notwithstanding the Companies' failure to fully respond to this directive, we find that information made publicly available by their parent entities provides ample evidence that the corporate leadership of the Companies overlaps or is closely associated with the corporate leadership of the Companies' parent entities and, ultimately, the Chinese government. In their response to the *Order to Show Cause*, the Companies identify the two directors of Pacific Networks and ComNet as Executive Directors of CITIC Tel as of the date of that filing.[229] The Companies, however, dismiss any significance of this overlap, stating that "neither Mr. Cai Da Wei nor Mr. Li Bing Chi, Esmond, the directors of the Companies, spend any significant time controlling the Companies' affairs, much less involving themselves in the Companies' day-to-day management, given that they are only required to make financial decisions for the Companies."[230] We reject the Companies' arguments and find no evidence in the record that the corporate powers conferred to the Companies' directors pursuant to their corporate governance documents include solely the ability to make financial decisions.[231] In fact, Pacific Networks' Bylaws set forth the powers of its directors, by which, {[ ]}[232] We observe that the {[} which the Companies describe as "the current limited liability company agreement for ComNet,"[233] {[ ]} by stating, with respect to the corporate governance documents, "these documents are typical of organizational documents for corporations and

[229] PN/CN June 1, 2020 Response, Exh. B; *see infra* para. 50 & note 239. Based on their June 1, 2020 filing, the Companies' corporate governance information shows that Pacific Networks, ComNet, and Pacific Choice International Limited have an identical two-person Board of Directors as of the date of that filing. PN/CN June 1, 2020 Response, Exhs. B and C. The Companies state that "[n]o other officers or senior officials are employed by" Pacific Networks and Pacific Choice International Limited. *Id.*, Exh. B at B-1; *id.*, Exh. C at C-1. The Companies identify one individual as "Officers and Other Senior Officials" of ComNet. *Id.*, Exh. B at B-2.

[230] PN/CN April 28, 2021 Reply at 71. The Companies further state that "[s]pecific approval by the Directors is required for opening and closing bank accounts, changes in bank signatories and other significant financial matters (such as mergers, acquisitions etc.)." *Id.* at 44-45. The Companies contend, however, that, "as is also often the case for corporations and LLCs, the Directors of both Companies have delegated day-to-day responsibility for management except for involvement in certain significant financial decisions, and . . . spend an insignificant amount of their time involved in the Companies' management and operation." *Id.* at 47.

[231] In the *Institution Order*, we directed Pacific Networks and ComNet to include in their response "a description and copy of any policies or agreements concerning Pacific Networks' and ComNet's corporate governance or decision making." *Institution Order*, 36 FCC Rcd at 6415, Appx. A. In their response, the Companies included "(1) the Articles of Incorporation and Bylaws for Pacific Networks and (2) the current limited liability company agreement for ComNet." PN/CN April 28, 2021 Reply at 46; *id.*, Business Confidential Exh. A.

[232] PN/CN April 28, 2021 Reply, Business Confidential Exh. A at A-12. Pacific Networks' Bylaws {[ ]} *Id.*, Business Confidential Exh. A at A-26.

Material set off by double brackets {[ ]} is confidential and is redacted from the public version of this document.

[233] *Id*. at 46.

[234] *Id*., Business Confidential Exh. A at A-28, A-40-A-41.

[235] *Id*., Business Confidential Exh. A at A-41.

LLCs, [and] do provide for the management of the business by their respective Directors."[236] Significantly, the Companies' 2009 LOA was executed by the Chairman of Pacific Networks and a "Director" of ComNet on behalf of the Companies.[237]

50. The record evidence and information made publicly available by the Companies' parent entities confirm that Mr. Cai Da Wei is on Pacific Networks' Board of Directors and has also served in various key positions at CITIC Tel, including as Chief Information Officer, Vice President, and presently, Executive Director and Chief Executive Officer.[238] The other Director of Pacific Networks and ComNet identified by the Companies, Mr. Li Bing Chi, Esmond, was Executive Director and Chief Financial Officer of CITIC Tel as of the Companies' June 1, 2020 filing, however, based on information made publicly available by CITIC Tel, he no longer holds those positions at CITIC Tel as of February 1, 2022.[239] Based on CITIC Tel's recent January 19, 2022 public announcement, a newly appointed Executive Director and Chief Financial Officer of CITIC Tel is or was also a director and officer of CITIC Pacific Limited, a "controlling shareholder" of CITIC Tel,[240] and was also part of the corporate leadership of CITIC Group Corporation and CITIC Limited.[241] Further, other individuals on CITIC Tel's

[236] *Id*. at 46-47. While the Companies state that they have provided "the current limited liability company agreement for ComNet," they do not explain {[

]} *See id*.; *see also id*., Business Confidential Exh. A at A-40-A-41. The Companies nonetheless identify two "Directors" and one "General Manager of Human Resources & Administration" as comprising the "officer and directors" of ComNet as of the Companies' June 1, 2020 filing. *See* PN/CN June 1, 2020 Response, Exh. B. {[

]} PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-8.

[237] 2009 LOA at 5.

[238] PN/CN June 1, 2020 Response, Exh. B; *see* CITIC Telecom International Holdings Limited, *About Us – Leadership*, https://www.citictel.com/about-us/leadership/ (last visited Mar. 13, 2022) (*CITIC Tel—Leadership*) (identifying "Mr. Cai Dawei" as "Executive Director and Chief Executive Officer of the Company"); CITIC Telecom International Holdings Limited, List of Directors and their Role and Function (Feb. 1, 2022), https://www1.hkexnews.hk/listedco/listconews/sehk/2022/0131/2022013100972.pdf (*CITIC Tel—List of Directors*) (identifying "Cai Dawei" as an "Executive Director[]" of CITIC Tel as of February 1, 2022). According to CITIC Tel's 2020 Annual Report, "[t]he Chief Executive Officer is responsible for the day-to-day management of the Group and the effective implementation of corporate strategy and policies." CITIC Telecom International Holdings Limited, Annual Report 2020 at 50 (Mar. 30, 2021), https://www1.hkexnews.hk/listedco/listconews/sehk/2021/0330/2021033001214.pdf (CITIC Tel 2020 Annual Report); *see id.* at ii (referring to CITIC Tel as "the 'Company', and together with its subsidiaries the 'Group'").

[239] PN/CN June 1, 2020 Response, Exh. B; CITIC Telecom International Holdings Limited, Changes to the Board at 1 (Jan. 19, 2022), https://www1.hkexnews.hk/listedco/listconews/sehk/2022/0119/2022011900176.pdf (*CITIC Tel—Changes to the Board*); *CITIC Tel—List of Directors*.

[240] *CITIC Tel—Changes to the Board* at 2. CITIC Pacific Limited is an entity incorporated in the British Virgin Islands that is included in the Companies' vertical chain of ownership. PN/CN June 1, 2020 Response, Exh. A (reflecting that CITIC Limited holds 100% ownership interest in CITIC Pacific Limited); *see* CITIC Pacific Limited, *About Us*, https://www.citicpacific.com/about-us (last visited Mar. 13, 2022) (stating that CITIC Pacific Limited is "[h]eadquartered in Hong Kong" and "is a wholly owned subsidiary of CITIC Limited (267.HK) which is listed on the Hong Kong stock exchange and one of China's largest conglomerates.").

[241] *CITIC Tel—Changes to the Board* at 1-2 (stating that CITIC Tel's newly appointed Executive Director and Chief Financial Officer, "prior to joining the Group, is a director, Vice President and Treasurer of CITIC Pacific Limited" and "was also the deputy director-general of the finance department of CITIC Group Corporation (the ultimate controlling shareholder of the Company), and the Vice President of the treasury department of CITIC Limited"); *CITIC Tel—Leadership* ("Mr. Luan Zhenjun has been an executive director and Chief Financial Officer of the Company since 1 February 2022. Prior to joining the Group, he is a director, Vice President and Treasurer of CITIC (continued….)

Board of Directors also hold or previously held positions in the corporate leadership of the company's parent entities, including CITIC Limited and CITIC Group Corporation.[242] For instance, one of the three Non-Executive Directors of CITIC Tel is currently Vice President of CITIC Group Corporation, CITIC Limited, and CITIC Corporation Limited.[243] An additional Non-Executive Director of CITIC Tel is a director of CITIC Pacific Limited and was also an executive director of CITIC Limited.[244] A third Non-Executive Director of CITIC Tel is a director of CITIC Pacific Limited and was also deputy director-general of the finance department of CITIC Group Corporation.[245] Notably, CITIC Tel publicly identifies CITIC Group Corporation and CITIC Limited as its "Major Shareholder."[246] Given the record of overlapping corporate leadership in the Companies' chain of ownership and the presence of a director of CITIC Tel on the Companies' Board of Directors, to the extent the Companies control their day-to-day business operations, it is highly likely that the Companies are not insulated from the influence of their parent entities or ultimately, the Chinese government.[247]

(Continued from previous page)
Pacific Limited ('CITIC Pacific', the controlling shareholder of the Company)."); *see supra* note 240 (discussing CITIC Pacific Limited); *see infra* note 317 (discussing CITIC Limited).

[242] *CITIC Tel—Leadership*; CITIC Tel 2020 Annual Report at 67.

[243] *CITIC Tel—Leadership*; CITIC Tel 2020 Annual Report at 67; CITIC Limited, *Senior Management*, https://www.citic.com/en/aboutus/senior_management/ (last visited Mar. 13, 2022) (*CITIC Limited Senior Management*); CITIC Group Corporation, *About CITIC—The Board of Directors and Senior Managements*, https://www.group.citic/en/About_CITIC/Directors_Senior/ (last visited Mar. 15, 2022) (*CITIC Group Corporation—Board of Directors and Senior Managements*) ("Personnel Resume"). CITIC Corporation Limited is an entity incorporated in the People's Republic of China that is included in the Companies' vertical chain of ownership. PN/CN June 1, 2020 Response, Exh. A (reflecting that CITIC Limited holds 100% ownership interest in CITIC Corporation Limited).

[244] *CITIC Tel—Leadership*; CITIC Tel 2020 Annual Report at 67.

[245] *CITIC Tel—Leadership*; CITIC Tel 2020 Annual Report at 67.

[246] CITIC Telecom International Holdings Limited, *Major Shareholder*, https://www.citictel.com/about-us/major-shareholder/ (last visited Mar. 13, 2022).

[247] Additionally, the Companies state that "Pacific Networks has the right as the sole member of ComNet to appoint both Directors" of ComNet, and "Pacific Choice International Limited ('Pacific Choice'), a British Virgin Islands corporation, has the right as sole shareholder of Pacific Networks to appoint both Directors" of Pacific Networks. PN/CN June 1, 2020 Response at 10. As discussed above, the Companies' corporate governance information as of their June 1, 2020 filing shows that ComNet, Pacific Networks, and Pacific Choice International Limited, the immediate parent of Pacific Networks, have an identical two-person Board of Directors; presently, one of the Directors, Mr. Cai Da Wei, is an Executive Director of CITIC Tel. PN/CN June 1, 2020 Response, Exhs. B and C; *see supra* notes 238, 239; *CITIC Tel—List of Directors* (identifying "Cai Dawei" as an "Executive Director[]" of CITIC Tel as of February 1, 2022). Given the totality of the circumstances reflected in the record, we view the power of one of CITIC Tel's directors to appoint the directors of the subsidiaries, ComNet, Pacific Networks, and Pacific Choice International Limited, as further evidence of control. *See* 47 CFR § 63.24, Note 1 to paragraph (d) ("Because the issue of control inherently involves issues of fact, it must be determined on a case-by-case basis and may vary with the circumstances presented by each case. The factors relevant to a determination of control in addition to equity ownership include, but are not limited to the following: power to constitute or appoint more than fifty percent of the board of directors or partnership management committee . . . ability to play an integral role in major management decisions of the licensee . . . .").

In the context of its broadcast ownership and attribution rules, the Commission has addressed concerns about the influence of officers and directors in detail. *See generally* 47 CFR § 73.3555, Note 2g (officers and directors of broadcast licensees hold a cognizable ownership interest); *Corporate Ownership Reporting and Disclosure by Broadcast Licensees*; *Amendment of Sections 73.35, 73.240 and 73.636 of the Commission's Rules Relating to Multiple Ownership of Standard, FM, and Television Broadcast Stations*; *Amendment of Sections 73.35, 73.240, 73.636 and 76.501 of the Commission's Rules relating to Multiple Ownership of AM, FM, and Television Stations*
(continued….)

51. *The Companies' Operations are Integrated with their Parent Entities' Global Operations which are Aligned with Chinese Government Policies*. Based on information that is made public by the Companies' parent entities, the Companies' operations are integrated with their parent entities' global operations and the Companies are more closely associated with them than is apparent in their disclosures to the Commission.[248] As we stated in the *Institution Order*, CITIC Tel's coverage map identifies ComNet as a "Branch,"[249] notwithstanding the Companies' claim that ComNet is a "small, independently-operated" company.[250] CITIC Tel describes itself as "an internet-oriented telecommunications enterprise providing comprehensive services,"[251] and identifies ComNet as one of its subsidiaries "[t]hrough" which it "provide[s] state-of-the-art one-stop comprehensive ICT services to [its] customers."[252] CITIC Tel also

(Continued from previous page)
and CATV Systems; *Reexamination of the Commission's Rules and Policies Regarding the Attribution of Ownership Interests in Broadcast, Cable Television and Newspaper Entities*, Report and Order, 97 F.C.C.2d 997, 1025, para. 58 (1984) (stating, with respect to attribution of officers and directors of corporate licensees or those of the licensee's parent corporations in the broadcast context, that "the potential influence over a licensee wielded by these individuals is significant and should be cognizable if the purposes of our multiple ownership rules are to be properly vindicated"); *Review of the Commission's Regulations Governing Attribution of Broadcast Interests*; *Review of the Commission's Regulations and Policies Affecting Investment in the Broadcast Industry*; *Reexamination of the Commission's Cross-Interest Policy*, Notice of Proposed Rulemaking, 10 FCC Rcd 3606, 3610-11, para. 6 (1995) (recognizing "the influence of officers and directors over a licensee's day-today activities") (citing *The Amendment of Sections 3.35, 3.240 and 3.636 of the Rules and Regulations Relating to Multiple Ownership of AM, FM and Television Broadcast Stations*, Report and Order, 18 F.C.C. 288 (1953)); *id.* at 3628, para. 47 (stating that special regulatory treatment for so called "passive investors" is conditioned on their not serving as officers or directors of the licensee corporation); *see also News Corporation and the DirectTV Group, Inc., Transferors, and Liberty Media Corporation, Transferee, for Authority to Transfer Control*, MB Docket No. 07-18, Memorandum Opinion and Order, 23 FCC Rcd 3265, 3284-86, para. 43 (2008) (discussing overlapping boards of directors).

[248] *See Institution Order*, 36 FCC Rcd at 6388-89, para. 32.

[249] CITIC Telecom International Holdings Limited, *Corporate Profile—Coverage Map*, https://www.citictel.com/about-us/corporate-profile/ (last visited Mar. 19, 2022); *see* CITIC Telecom International Holdings Limited, *ComNet*, https://www.citictel.com/subsidiary/%e4%bf%a1%e9%80%9a%e9%9b%bb%e8%a9%b1-comnet/ (last visited Mar. 14, 2022) (*CITIC Tel—ComNet*); *Institution Order*, 36 FCC Rcd at 6388, para. 32 (citing *Corporate Profile—Coverage Map*; *CITIC Tel—ComNet*; CITIC Telecom International Holdings Limited, An Internet-Oriented Integrated Telecom & ICT Leader—CITIC Telecom International Company Profile at 9 (Sept. 2020) ("Global Coverage: Unique Edge in the 'Belt and Road' Regions"), https://www.citictel.com/wp-content/uploads/2020/09/CITIC-Telecom-International_Company-Profile-2020-September-eng.pdf).

[250] *See* PN/CN June 1, 2020 Response at 26.

[251] CITIC Tel 2020 Annual Report at ii; CITIC Telecom International Holdings Limited, *Corporate Profile*, https://www.citictel.com/about-us/corporate-profile/ (last visited Mar. 14, 2022) (*CITIC Tel—Corporate Profile*). CITIC Tel states that it is "one of the largest telecommunications hubs in Asia Pacific." CITIC Tel 2020 Annual Report at ii; *CITIC Tel—Corporate Profile*. Further, according to CITIC Tel, it "is a pioneer in Mainland China's international telecommunications business and an important international business partner of Mainland China's three major operators." CITIC Telecom International Holdings Limited, *Our Partners*, https://www.citictel.com/about-us/partnership/ (last visited Mar. 14, 2022); CITIC Telecom International Holdings Limited, *Products and Services—Carrier*, https://www.citictel.com/products_services/carrier/ (last visited Mar. 19, 2022) (identifying "China Mobile," "China Unicom," and "China Telecom" as "Carrier customer").

[252] CITIC Telecom International Holdings Limited, *Our Subsidiaries*, https://www.citictel.com/about-us/subsidiary-companies/ (last visited Mar. 4, 2022) (*CITIC Tel—Subsidiaries*); *see supra* note 249. CITIC Tel publicly states, "[t]he Group is connecting more than 600 operators around the world, and serving over 40,000 enterprise customers, with network, business and branches all over the world." *CITIC Tel—Subsidiaries*. Additionally, we note that CITIC Tel identifies one of its "Strategy" as "New Market: Expand from mainland China, Hong Kong and Macau to Asia Pacific, Europe, the US and global market." *CITIC Tel— Corporate Profile*; *see* CITIC Telecom International Holdings Limited, An Internet-Oriented Integrated Telecom & ICT Leader—CITIC Telecom International Company
(continued….)

publicly identifies one of its "Mission[s]" as "[r]ooted in Mainland China, taking Hong Kong and Macau as the base and connection, providing communications and ICT services with global coverage,"[253] and states that it "also has unique coverage in the 'Belt and Road' region."[254] Notably, CITIC Tel has described its goals as aligned with China's national policies,[255] stating that "[t]he nation's '14th Five-Year

(Continued from previous page)
Profile at 7 (Aug. 2021), https://www.citictel.com/wp-content/uploads/2021/08/CITIC-Telecom-International_Company-Profile-2021-August-Eng.pdf (CITIC Tel 2021 International Company Profile) (displaying "One stop Integrated Telecom and ICT Product Portfolio" and identifying ComNet in relation to "Consumer (Overseas Chinese)"); *id.* at 9 (displaying "Global Coverage: Unique Edge in the 'Belt and Road' Regions" and identifying ComNet as "Original Coverage"); CITIC Telecom International Holdings Limited, *Products and Services*, https://www.citictel.com/products-and-services/ (last visited Mar. 19, 2022) ("In recent years, the Group has extended its footprint to the 'Belt and Road' regions in Southeast Asia, Central Asia, Central and Eastern Europe. Along with our existing operations in Greater China, Asia Pacific, Western Europe and North America, we are able to provide one-stop, cross-regional and end-to-end comprehensive communications and ICT services to our customers."). *See infra* para. 61 and note 327 (discussing Belt and Road Initiative).

[253] CITIC Tel 2020 Annual Report at ii; *see CITIC Tel—Corporate Profile*; CITIC Telecom International Holdings Limited, Interim Report 2021 at 1 (Sept. 10, 2021), https://www1.hkexnews hk/listedco/listconews/sehk/2021/0910/2021091000454.pdf (CITIC Tel 2021 Interim Report); *Institution Order*, 36 FCC Rcd at 6388, para. 32 (citing *CITIC Tel—Corporate Profile*); CITIC Telecom International Holdings Limited, Interim Report 2020, https://www.citictel.com/wp-content/uploads/2020/09/e1883_20200908.pdf.

[254] CITIC Telecom International Holdings Limited, *Message from the Chairman*, https://www.citictel.com/about-us/chairmans-statement/ (last visited Mar. 14, 2022); *see* CITIC Tel 2021 International Company Profile at 3, 9; *Institution Order*, 36 FCC Rcd at 6388-89, para. 32 (citing *Message from the Chairman*). *See infra* para. 61 and note 327 (discussing the leadership of the Chinese Communist Party over the People's Liberation Army and pursuit of the Belt and Road Initiative).

[255] *See, e.g.*, CITIC Telecom International Holdings Limited, Annual Report 2019 at 15 (Mar. 27, 2020), https://www1.hkexnews hk/listedco/listconews/sehk/2020/0327/2020032700911.pdf (CITIC Tel 2019 Annual Report). According to CITIC Tel, "[i]n tandem with the national strategic initiatives of the 'Belt and Road' and 'Guangdong-Hong Kong-Macao Greater Bay Area', the Group will step up its expansion to the international market, through Hong Kong and Macau as bases and bridges with its solid foundation in the Mainland China market." CITIC Telecom International Holdings Limited, *CITIC Telecom Announces 2019 Annual Results, Profit Attributable to Equity Shareholders Exceeds HK$1 Billion Up 5.4% Year-on-Year Total Dividends Increase by 11.1% Year-on-Year to HK20.0 Cents per Share* (Mar. 3, 2020), https://www.citictel.com/news_releases/citic-telecom-announces-2019-annual-result%ef%bc%8cprofit-attributable-to-equity-shareholders-exceeds-hk1-billion-up-5-4-year-on-year-total-dividends-increase-by-11-1-year-on-year-to-hk20-0-cents-per/; *see* CITIC Tel 2019 Annual Report at 15; CITIC Tel 2021 Interim Report at 7 ("The Group actively positioned itself in major national development plans such as 'Belt and Road' and Guangdong-Hong Kong-Macao Greater Bay Area with the implementation of a new development philosophy . . . ."); *see infra* para. 61 & note 327 (discussing Belt and Road Initiative); *see* State Council of the People's Republic of China, *Transport to play key role in Bay Area* (May 17, 2021), http://english.www.gov.cn/news/topnews/202105/17/content_WS60a1c118c6d0df57f98d99a0.html; State Council of the People's Republic of China, *Vice-premier stresses developing major Greater Bay Area cooperation platforms* (Apr. 23, 2021), http://english.www.gov.cn/statecouncil/hanzheng/202104/23/content_WS6082ad3cc6d0df57f98d8718.html. CITIC Tel's 2021 "CITIC Telecom International Company Profile" displays CITIC Tel's "Global Coverage" in the "Belt and Road Regions," which features coverage associated with the "Digital Silk Road." CITIC Tel 2021 International Company Profile at 9; *see* State Council of the People's Republic of China, *Digital Silk Road linked to "Net Plus"* (Sept. 8, 2015), https://english.www.gov.cn/news/top_news/2015/12/24/content_281475259901640 htm (displaying news article from China Daily stating, among other things, "Internet-based businesses and media have been asked to actively engage in the Belt and Road Initiative by building a 'digital Silk Road' and helping to upgrade traditional industries within and beyond China's borders" and "Qu Yingpu, deputy editor-in-chief of China Daily, said the country's Internet media could play an 'irreplaceable' role in promoting dialogue between different civilizations and communications between various nations."); Zhao Huanxin, *Web companies asked to support "digital Silk Road,"*
(continued….)

Plan' blueprint has indicated the future direction of the Group's development."[256] Similarly, CITIC Limited and CITIC Group Corporation have publicly affirmed their support of these Chinese government policies.[257] Further, CITIC Tel states that it "is the InfoComm sector arm under CITIC Limited."[258] Moreover, in 2017, a Vice President of CITIC Group Corporation and CITIC Limited described CITIC Tel as "'the flagship of CITIC Group in the information service sector'" and "'an important investment vehicle of the Group playing a crucial role in bringing synergies to and to full play the integrated advantages," and "[t]he Group will also spare no effort in supporting the development of CITIC Telecom.'"[259]

(Continued from previous page)
China Daily (Sept. 8, 2015), http://www.chinadaily.com.cn/business/2015chinaarabforum/2015-09/08/content_21823475.htm.

[256] CITIC Tel 2020 Annual Report at 15; *see id.* at ii (referring to CITIC Tel as "the 'Company', and together with its subsidiaries the 'Group'"). *See* State Council of the People's Republic of China, *China to advance major programs in 14th Five-Year Plan to harness key role of effective investment* (June 9, 2021), http://english.www.gov.cn/premier/news/202106/09/content_WS60c0caeac6d0df57f98dafcb html ("China will advance the implementation of major programs set out in the Outline of the 14th Five-Year Plan, to better tap the key role of effective investment, the State Council's executive meeting chaired by Premier Li Keqiang decided on June 9. The major programs span a series of key areas, including scientific and technological advances, infrastructural facilities, environmental protection, people's livelihoods and cultural heritage, among others."); U.S.-China Economic and Security Review Commission, Economics and Trade Bulletin (Apr. 30, 2021), https://www.uscc.gov/sites/default/files/2021-04/April_2021_Trade_Bulletin.pdf (USCC April 30, 2021 Bulletin) ("14th Five-Year Plan Sets Vision for 2021–2025 and Beyond").

[257] *See e.g.*, Li Xiang, *CITIC deepens backing for B&R*, China Daily (June 5, 2017), https://www.chinadaily.com.cn/kindle/2017-06/05/content_29622873.htm (discussing, "State-owned CITIC Group Corporation said it will continue to boost financing of and investment in, infrastructure projects related to the Belt and Road Initiative" and noting that the Chairman of CITIC Group Corporation stated in an interview, "'CITIC Group has encouraged its financial and non-financial units to join hands in advancing the Belt and Road Initiative . . . .'"); State Council of the People's Republic of China, *Belt and Road to get $113b in CITIC financing* (June 26, 2015), http://english.www.gov.cn/news/top_news/2015/06/26/content_281475134729436 htm (displaying article published in the China Daily stating, among other things, "subsidiaries of the State-owned CITIC Group Corp plan to support the country's Belt and Road Initiative"); CITIC Limited, 2019 Annual Report at 139 (Apr. 21, 2020), https://www1.hkexnews hk/listedco/listconews/sehk/2020/0421/2020042100994.pdf (CITIC Limited 2019 Annual Report) (stating, "[t]o support the 'Belt and Road' initiatives, we adopted an on-site training approach for the first time, focusing on training our employees in Kazakhstan to learn the latest national policies and company requirements" and "[t]o realise the social responsibility of a state-owned enterprise, we organised job rotation for our staff in Hong Kong and Macau for four consecutive years to deepen their understanding of the Group and in mainland China as well as to promote mutual exchange"); CITIC Limited, Annual Report 2020 at 4 (Apr. 21, 2021), https://www1.hkexnews hk/listedco/listconews/sehk/2021/0421/2021042100516.pdf (CITIC Limited 2020 Annual Report) ("In alignment with China's 14th Five-Year Plan, and to adapt to the increasingly complex operating environment, CITIC has outlined an updated development strategy focused on comprehensive financial services, advanced intelligent manufacturing, advanced materials, new consumption and new-type urbanisation").

[258] CITIC Tel 2021 International Company Profile at 3. CITIC Limited, an indirect parent entity of CITIC Tel, states that "CITIC Limited provides information services through two subsidiaries" which includes "CITIC Telecom International." CITIC Limited 2019 Annual Report 2019 at 52.

[259] CITIC Telecom International Holdings Limited, CITIC Telecom Celebrates 10th Listing Anniversary at 1 (Oct. 27, 2017), https://www.citictel.com/wp-content/uploads/2018/10/CITIC-Telecom-10th-IPO-Anniversary_E_20171026_Final.pdf (*CITIC Tel 10th Listing Anniversary*); CITIC Telecom International Holdings Limited, *10th Listing Anniversary of CITIC Telecom International*, https://www.citictel.com/story/%E4%B8%AD%E4%BF%A1%E5%9C%8B%E9%9A%9B%E9%9B%BB%E8%A8%8A%E4%B8%8A%E5%B8%82%E5%8D%81%E9%80%B1%E5%B9%B4%E8%AA%8C%E6%85%B6/ (*10th Listing Anniversary of CITIC Tel*) (last visited Mar. 14, 2022); *Institution Order*, 36 FCC Rcd at 6389, para. 32 (citing *CITIC Tel 10th Listing Anniversary*; *10th Listing Anniversary of CITIC Tel*). This Vice President of CITIC Group Corporation and CITIC Limited further stated, "'CITIC Group is seeking to transform itself through
(continued….)

52. *CITIC Tel's Information Security Policy.* Importantly, record evidence and information made publicly available by the Companies' parent entities support the national security and law enforcement concerns associated with the Companies' ownership and control in light of the Companies' additional disclosures regarding CITIC Tel's oversight of and involvement in critical matters concerning the security and protection of U.S. records. In their response to the *Order to Show Cause*, the Companies assert that CITIC Tel "do[es] not assess or require changes in the Companies' technical or network operations."[260] In the *Institution Order*, we indicated that the PSI Report contradicts this statement by stating that "[CITIC Tel] also guides ComNet on its information security policies,"[261] and that "ComNet maintains a company-specific policy" that was drafted based on CITIC Tel's "guidance."[262] In their response to the *Institution Order*, the Companies state they "should have clarified that while the Companies' indirect owners may not require that specific technical decisions be made on a day-to-day basis, the Companies *observe* guidance from CITIC Tel regarding network security."[263] The Companies further state that "CITIC Tel has adopted policies related to information technology, security and access that have been shared with the Companies"[264] but "[t]he Companies are expected to implement their own policies and controls with reference to those guidelines."[265] The Companies state that "[t]he guidance

(Continued from previous page)
developing "Internet+" communication business and emerging strategic industries.'" *CITIC Tel 10th Listing Anniversary* at 1. Furthermore, a former Executive Director and Chief Executive Officer of CITIC Tel also stated, "'[l]ooking ahead, we will build on the past to explore and to innovate, with a vision of becoming "an internet-oriented telecommunications company".'" *CITIC Tel 10th Listing Anniversary* at 2; *see CITIC Tel—Corporate Profile*.

[260] PN CN June 1, 2020 Response at 11 (stating, "[t]he financial positions of Pacific Networks and ComNet are routinely reviewed by CITIC Tel, but they do not assess or require changes in the Companies' technical or network operations").

[261] PSI Report at 95-96 (citing Briefing with ComNet (Apr. 13, 2020)); *Institution Order*, 36 FCC Rcd at 6385, para. 26 (quoting PSI Report at 95-96).

[262] PSI Report at 96 (citing Briefing with ComNet (Apr. 13, 2020)); *Institution Order*, 36 FCC Rcd at 6385, para. 26 (quoting PSI Report at 96). As we stated in the *Institution Order* the record shows that the Companies informed DOJ in a December 13, 2017 Letter, that {[

]} PN/CN June 1, 2020 Response, Business Confidential Exh. K at 21; *Institution Order*, 36 FCC Rcd at 6385-86, para. 27 (quoting PN/CN June 1, 2020 Response, Business Confidential Exh. K at 21). According to the December 13, 2017 Letter, {[

]} PN CN June 1, 2020 Response, Business Confidential, Exh. K at 21-22; *Institution Order*, 36 FCC Rcd at 6386, para. 27 (quoting PN/CN June 1, 2020 Response, Business Confidential, Exh. K at 21-22). {[

]} PN CN June 1, 2020 Response, Business Confidential, Exh. K at 22; *id.*, Exh. A; *Institution Order*, 36 FCC Rcd at 6386, para. 27, n.119 (citing PN/CN June 1, 2020 Response, Exhs. A, K). *See* PN/CN June 1, 2020 Response, Business Confidential, Exh. K at 84 ({[

]}).

[263] PN/CN April 28, 2021 Reply at 69-70 (emphasis added). Such admission further demonstrates that the Companies omitted critical information in their response to the *Order to Show Cause. See infra* Section III.B.3.

[264] PN/CN April 28, 2021 Reply at 44.

[265] *Id*. The Companies state, "[t]his fact, however, has been long known to the United States government, since the Companies provided a full set of the applicable policies in 2009 to Team Telecom as required by the 2009 Letter of Assurance. This policy was titled the 'Pacific Networks Corp. IT Security Policy,' but was derived from the then current CITIC Tel Information Technology Security Policy. As the [*Institution Order*] notes, {[

(continued….)

provided to the Companies by the CITIC Tel Information Security Policy has thus been a part of the ComNet's information security approach since Pacific Networks acquired ComNet."[266] The Companies contend, however, that "any corporate entity with multiple affiliates involved in handling communications and information technology would want to avoid the inefficiencies and increased chance of compromise created by using different policies."[267]

53. Contrary to the Companies' suggestion that their compliance with the CITIC Tel Information Security Policy is not "relevant (much less material) to the question of 'control' over operations,"[268] we find that the record shows how integrated ComNet's and Pacific Networks' operations—{[ ]}—are with that of their indirect parent entity, CITIC Tel, and its subsidiaries, {[ ]} and how closely ComNet and Pacific Networks coordinate with these entities.[269] Based on our review, the record

(Continued from previous page)

]} *Id.* (citing *Institution Order*, 36 FCC Rcd at 6385-86, para. 27).

[266] *Id.* at 68.

[267] *Id*. The Companies argue that "the promulgation of consistent data security policies across affiliated entities does not somehow change ComNet from having independence in its day-to-day operations to having all of its decisions dictated by indirect owners." *Id.* They also argue that "[t]hese policies are comparable to other corporate information security policies," and "these policies provide the kind of protections and processes that one would expect to apply to any telecommunications or information service provider, and do so in a way that allows local management flexibility in implementation." *Id.* at 51, 68. The Companies state, "[a]s noted by the [*Institution Order*], {[

]} *Id.* at 69 (citing *Institution Order*, 36 FCC Rcd at 6385-86, para. 27).

[268] *See id.*at 66; *see also id.* at 67-68; *Institution Order*, 36 FCC Rcd at 6385-86, para. 27 (addressing PN/CN June 1, 2020 Response, Business Confidential Exh. K at 21-22); PN/CN June 1, 2020 Response, Business Confidential Exh. K at 21 ({[

]}).

[269] {[

(continued….)

evidence demonstrates that the Companies do not simply "observe" CITIC Tel's Information Security Policy,[270] as they indicate that "[t]he guidance provided to the Companies by the CITIC Tel Information Security Policy has thus been a part of ComNet's information security approach since Pacific Networks acquired ComNet"[271] and that the Pacific Networks Corp. IT Security Policy "was succeeded by the CITIC Tel Information Security Policy" in 2017.[272] In fact, based on their own admissions, as discussed below, the Companies work closely with their indirect parent entity and {[ ]} concerning access to U.S. customer records. With respect to ComNet's Retail Calling Card service, the Companies state that ComNet "manage[s]" access to U.S. records.[273] However, with respect to ComNet's Wholesale IDD service and Pacific Networks' MPLS VPN service, the Companies state that they manage access to these U.S. records by "coordinat[ing]" with CITIC Tel and with {[ ]}[274] Significantly, the Companies did not disclose any further information on this joint coordination process, including who has the final decision-making authority in granting access to those records.[275] Based on the record, {[ ]}[277]

54. The Companies further state, with respect to Pacific Networks' MPLS VPN service, that "individuals employed by {[ ]}, a subsidiary of [CITIC Tel], have access to U.S. customer records to provide support and billing" and that {[ ]} provides first tier

(Continued from previous page)

]} *See* PN/CN April 28, 2021 Reply at 49-51, 59. 72; *see infra* Section III.B.2.

[270] *See* PN/CN April 28, 2021 Reply at 69-70 (stating, "the Companies should have clarified that while the Companies' indirect owners may not require that specific technical decisions be made on a day-to-day basis, the Companies observe guidance from CITIC Tel regarding network security.")

[271] *Id*. at 68.

[272] *Id*., Declaration of Li Ying (Linda) Peng.

[273] *Id*. at 49.

[274] *Id*. at 47-50.

[275] The Companies state, with respect to {[ ]} associated with ComNet's Wholesale IDD service, "[f]or this service, access to records is coordinated by CITIC Tel according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy." *Id.* at 47-48. The Companies state, with respect to U.S. customer records associated with Pacific Networks' MPLS VPN service, "[f]or this service, access to records is coordinated by {[ ]} according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy." *Id*. at 49-50.

[276] *Id*. at 47-50; *see infra* para. 56.

[277] PN/CN April 28, 2021 Reply at 59; *see infra* para. 57.

support for Pacific Networks' MPLS VPN service."[278] The Companies also state that "[b]oth of these services are provided to Pacific Networks pursuant to a services contract with {[ ]}, a subsidiary of {[ ]}[279] In fact, based on the Companies' description of the arrangement involving Pacific Networks' MPLS VPN service and the services contract, {[

]}"[281] The services contract also shows that {[

]}[282] As discussed below, the services contract further demonstrates how closely integrated Pacific Networks' operations are with that of its affiliate and, moreover, underscores the national security and law enforcement risks concerning access to and protection of U.S. customer records.[283]

55. Like similarly situated service providers, the Companies may follow their parent entities' IT policies, including information security. Unlike many other providers, however, the Companies manage access to U.S. customer records by "coordinat[ing]" with their indirect parent entity and {[ ]} and are indirectly majority-owned and controlled by the Chinese government, with significant legal obligations imposed on the Companies, as discussed below.[284] A close reading of the CITIC Tel Information Security Policy—particularly those provisions that the Companies state govern "all access to U.S. records"[285]—further highlights the close association between the Companies, CITIC Tel, and

[278] PN/CN April 28, 2021 Reply at 72.

[279] *Id*.; *but see id.* at 49 (responding specifically to the Commission's inquiry involving access to U.S. customer records by stating, {[

]}); *id.* at 47. According to the Companies, "[n]either of these subsidiaries is a direct or indirect owner of either of the Companies. They are thus affiliates, not owners, of Pacific Networks." *Id.* at 72.

[280] *See id.* at 72; *id.*, Business Confidential Exh. J-2-J-3 ({[

]}) (emphasis added).

[281] *Id*., Business Confidential Exh. J at J-2.

[282] *Id*., Business Confidential Exh. J at J-3.

[283] *See infra* para. 107.

[284] PN/CN April 28, 2021 Reply at 47-50; *see infra* paras. 63-73.

[285] PN/CN April 28, 2021 Reply at 51 (stating, "all access to U.S. records is governed by Sections 6 and 10 of the current version of the CITIC Tel Information Security Policy"); *id.*, at 47-51; *see id.*, Business Confidential Exh. B. The Companies state that "[t]his is the current version of the policy provided to Team Telecom in 2017 and included in Exhibit K in the [Order to Show Cause] Response." *Id*. at 48, n.107. The Companies state that they "provided a full set of the applicable policies in 2009 to Team Telecom as required by the 2009 Letter of Assurance. This policy was titled the 'Pacific Networks Corp. IT Security Policy,' but was derived from the then current CITIC Tel

(continued….)

{[ ]} and ultimately, the Companies' vulnerability to exploitation, influence, and control by the Chinese government.[286]

56. Significantly, and most concerning here, the record shows that CITIC Tel {[ ]}[287] and CITIC Tel and {[ ]}[288] In their response to the *Institution Order*, the Companies state that {[

(Continued from previous page)
Information Technology Security Policy. As the [*Institution Order*] notes, {[ ]} *Id*. at 44 (citing *Institution Order,* 36 FCC Rcd at 6385-86, para. 27).

[286] As discussed in Section III.C., we find that the CITIC Tel Information Security Policy is not a "practicable measure[]" that would "prevent unauthorized access to, or disclosure of the content of communications or U.S. records." *See infra* Section III.C. (Termination of International Section 214 Authorizations); 2009 LOA at 2.

[287] *See supra* note 262; PN/CN June 1, 2020 Response, Exh. K at 21; PN/CN April 28, 2021 Reply at 67-68 (citing *Institution Order*, 36 FCC Rcd at 6385-86, para. 27); *Institution Order*, 36 FCC Rcd at 6385-86, para. 27.

[288] PN/CN April 28, 2021 Reply at 47-51, 59; *id.,* Business Confidential Exh. J at J-2-J-3; PN/CN June 1, 2020 Response, Business Confidential Exh. D at D-2, D-4; *see infra* Section III.C. {[

]}

]}[295] The Companies' description of the arrangements and the services agreement concerning Pacific Networks' MPLS VPN service show, {[

]}[296] In addition, with respect to ComNet's Retail Calling Card service, {[

[289] PN/CN April 28, 2021 Reply at 69.

[290] PN/CN June 1, 2020 Response, Business Confidential, Exh. K at 21-22.

[291] PN/CN April 28, 2021 Reply at 51; *see id.* at 47-50.

[292] *Id.* at 47-48. According to the Companies, {[

]} *Id*. at 47.

[293] *Id*. at 48. In a July 6, 2015 Letter to DHS, the Companies {[

]} PN/CN June 1, 2020 Response, Business Confidential Exh. K at 17.

[294] PN/CN April 28, 2021 Reply at 49. The Companies state that {[

]} *Id*.

[295] *Id.*

[296] *Id.* at 72; *id*., Business Confidential Exh. J at J-2-J-3. According to the Companies, "individuals employed by {[ ]}, a subsidiary of [CITIC Tel], have access to U.S. customer records to provide support and billing." *Id.* at 72. Additionally, the Companies state that {[ ]} provides first tier support for Pacific Networks' MPLS VPN service. Both of these services are provided to Pacific Networks pursuant to a services contract with {[ ]}, a subsidiary of {[ ]} *Id.*; *see id.*, Business Confidential Exh. J.

[297] *Id*. at 48.

]}[298]

57. The record shows that CITIC Tel further has oversight over the Companies through the CITIC Tel Information Security Policy, as the policy also governs CITIC Tel's and {[ ]} access to ComNet's and Pacific Networks' systems, respectively.[299] With respect to ComNet, the Companies state that "CITIC Tel's SOC in Hong Kong provides first tier support for ComNet's Wholesale IDD service, Retail Calling Card service, International SMS Service and VoIP services" and "[a]ll access to ComNet's systems through the SOC is governed by the CITIC Tel Information Security Policy."[300] The Companies add that "[o]nly the authorized monitoring system and engineer team in Hong Kong can monitor and manage the equipment in ComNet's Los Angeles data center via MPLS VPN."[301] With respect to Pacific Networks, the Companies state that "[a]ll access to Pacific Networks' systems through the {[ ]} is governed by the CITIC Tel Information Security Policy,"[302] and "[o]nly the authorized monitoring system and engineer team in {[ ]} can monitor and manage the equipment in Pacific Networks' facilities via a private MPLS network."[303] We find that this evidence in the record demonstrates the Companies' close coordination with CITIC Tel, an indirect parent entity, and with {[ ]} in critical matters involving access to U.S. customer records and access to the Companies' systems in the United States. This record evidence raises significant national security and law enforcement concerns, especially given that our review of the CITIC Tel Information Security Policy shows that the terms of the policy {[ ]}[304]

58. *The Companies' Indirect Parent Entities Have Ties to the Chinese Communist Party and the Chinese Government.* Significantly, despite the directives in the *Order to Show Cause* and the *Institution Order*,[305] the Companies failed to provide sufficient information regarding the ties of their parent entities' corporate leadership with the Chinese Communist Party. In their response to the *Order to Show Cause*, the Companies state that, with respect to "directors, officers and other senior management officials" of Pacific Networks, ComNet, and Pacific Choice International Limited, the direct parent entity of Pacific Networks, "none have any prior employment with the Chinese government or have had any affiliations with the Chinese Communist Party or the Chinese government."[306] The Companies, however,

[298] *Id*. at 49.

[299] *Id.* at 59.

[300] *Id*. The Companies did not identify the full name of the acronym, "SOC," in this statement and instead referred generally to the CITIC Tel Information Security Policy. *Id.* {[ ]} the Companies refer to "Service Operations Center" in their response. *Id*., Exh. B at B-17, B-62; *id.* at 65 (referring to "CITIC Tel's Hong Kong Service Operations Center ('SOC')").

[301] *Id*. at 59.

[302] *Id*. The Companies state, "this Network Operations Center that provides support to Pacific Networks is a different facility from the SOC that provides support to ComNet. The 'NOC' identified in the PSI Report, *see* PSI Report at 96, is the CITIC Tel SOC identified above and distinguished from this facility." *Id.*, n.114. *See also* PSI Report at 96 ("ComNet leverages [CITIC Tel's] network operations center ('NOC'), located in Hong Kong, for 'first tier monitoring' against cyber incidents or disruptions.").

[303] *Id*. at 59.

[304] *See infra* Section III.C.

[305] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9; *Institution Order*, 36 FCC Rcd at 6415, Appx. A.

[306] PN/CN June 1, 2020 Response at 11-12; *Institution Order*, 36 FCC Rcd at 6390, para. 33 (quoting PN/CN June 1, 2020 Response at 11-12).

did not disclose such information pertaining to their other parent entities. The Companies then failed to respond to a similar directive in the *Institution Order*, stating only that "[a] list of the members of CITIC Group's Group Party Committee, Board of Directors, Board of Supervisors, and Senior Management, together with biographies for each of them, can be found at" CITIC Group Corporation's website.[307]

59. Notwithstanding the Companies' failure to fully respond to this directive, information that the Companies' indirect parent entities have made publicly available on their websites provides ample evidence that the Companies' indirect parent entities have irrefutable ties with the Chinese Communist Party and, consequently, the Chinese government. Importantly, based on such publicly available information, several individuals in the corporate leadership of the Companies' indirect parent entities previously held positions in the Chinese government. For instance, CITIC Tel's Chairman of the Board of Directors "serv[ed] a substantial period of time in the government of the People's Republic of China (the 'PRC') in which Mr. Xin was involved in the administration of science, technology information and economics."[308] In addition, several individuals on the Board of Directors of CITIC Group Corporation and/or CITIC Limited held positions of employment with the Chinese government,[309] including the Ministry of Finance, which is the government entity that wholly owns CITIC Group Corporation.[310] These relationships between the Companies' indirect parent entities and the Chinese government are further underscored by the ties of the corporate leadership of those entities with the Chinese Communist Party.

60. In fact, upon the appointment of its previous corporate leadership by the Central Party Committee[311] and the State Council,[312] CITIC Group Corporation—the ultimate parent of the Companies—publicly stated, "[t]he readjustment is a normal exchange of cadre members and shows the great attention and concern paid by the Central government to CITIC" and "Comrade Chang Zhenming, with firm political positions and an overall view, has always been fully implementing all principles and polices of the state Council and the decisions of the Party Committee of the group."[313] According to

[307] PN/CN April 28, 2021 Reply at 46 (displaying a weblink, https://www.group.citic/en/About_CITIC/Directors_Senior/).

[308] *CITIC Tel— Leadership*; CITIC Tel 2020 Annual Report at 66.

[309] Based on information made publicly available by these entities, the Chairman of CITIC Group Corporation and CITIC Limited was the Vice Governor of Sichuan province. *CITIC Group Corporation—Board of Directors and Senior Management*; CITIC Limited, *Board of Directors*, https://www.citic.com/en/aboutus/board_of_directors/ (last visited Mar. 15, 2022) (*CITIC Limited Board of Directors*).

[310] Four such directors, who are both "Equity Director[s]" of CITIC Group Corporation and "Non-Executive Directors" of CITIC Limited, previously held positions of employment at the Ministry of Finance. *CITIC Group Corporation—Board of Directors and Senior Management*; *CITIC Limited Board of Directors*.

[311] Based on the Revised Constitution of the Communist Party of China, revised and adopted on October 24, 2017 at the 19th National Congress of the Communist Party of China, "[t]he highest leading bodies of the Party are the National Congress and the Central Committee which it elects." Executive Branch CTA Recommendation, Exh. 114 at EB-2397, Constitution of the Communist Party of China, Revised and adopted at the 19th National Congress of the Communist Party of China, Article 10 (Oct. 24, 2017), http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf (Revised Constitution of the Communist Party of China).

[312] According to the Congressional-Executive Commission on the People's Republic of China, established by Congress in October 2000, "[t]he State Council executes laws and supervises the government bureaucracy and thus carries out the administrative functions of the Chinese government." Congressional-Executive Commission on China, *China's State Organizational Structure*, https://www.cecc.gov/chinas-state-organizational-structure#sc (last visited Mar. 15, 2022). CITIC Group Corporation was established upon the approval of the State Council. *CITIC Group Corporation Corporate Governance and Risk Management*; CITIC Group 2018 U.S. Resolution Plan at 7.

[313] CITIC Group Corporation, *The Central Party Committee and the State Council Readjust the leadership of CIT* (Dec. 29, 2010), https://www.group.citic/en/2010/News_1229/20 html; *id.* ("Under the new leadership, CITIC

(continued….)

CITIC Group Corporation's website, the current Chairman and an Executive Director is "Party Secretary" of CITIC Group Corporation.[314] As discussed in the *Institution Order*, CITIC Group Corporation has a Chinese Communist Party organization ("Group Party Committee") within its corporate leadership.[315] CITIC Group Corporation's corporate governance information identifies the three Executive Directors of the entity as "Party Secretary," "Deputy Party Secretary," and "Party Committee Member," respectively, of the Group Party Committee.[316] These Executive Directors of CITIC Group Corporation are also the three Executive Directors of CITIC Limited, an indirect parent of the Companies.[317] In addition, the President (also an Executive Director) and all of the five Vice Presidents (including an Executive Director) of CITIC Group Corporation are identified as part of the ultimate parent entity's Group Party Committee.[318] One of the Vice Presidents and "Party Committee Member" of CITIC Group Corporation is also a Non-Executive Director of CITIC Tel.[319] Further, an individual identified as a "Deputy Party Secretary" and the six individuals identified as a "Party Committee Member" of CITIC Group

(Continued from previous page)
Group will continue to hold high the great banner of Deng Xiaoping Theory and the important Thoughts of Three Represents, further implement the Scientific Approach to Development, closely unite the Central Party Committee with President Hu Jintao at its core. We will live up to the expectation of the Central Committee to keep being united and innovated, striving for developing CITIC to be a world-class conglomerate with clear overall strengths and core competencies and leading in its fields so as to make greater contribution to economic and social development of our country.").

[314] *CITIC Group Corporation—Board of Directors and Senior Management*.

[315] *Id.*; *Institution Order*, 36 FCC Rcd at 6390, para. 33 (citing *CITIC Group Corporation—Board of Directors and Senior Management*; Michael Forsythe, *CITIC Securities, a Pillar of Finance in China, Is in Beijing's Cross Hairs* (Sept. 17, 2015), https://www nytimes.com/2015/09/18/business/dealbook/citic-securities-investigation-china.html (stating, "the CITIC Group, is one of the most prominent companies in China. Founded in 1979, the CITIC Group originally served as China's investment arm when the country was just starting to open its economy to the outside world. The sons and daughters of many of the Communist Party's senior officials in the 1980s, the so-called eight immortals, served as top executives at the conglomerate."); Yasuo Awai, *China's Citic Leading Reform of State-Owned Companies* (Nov. 29, 2014), https://asia nikkei.com/Business/China-s-Citic-leading-reform-of-state-owned-companies (stating, "Citic is a publicly traded conglomerate that wears the face of a private company, but in reality it is also a strategic arm of the Chinese government and is close to the country's leadership."); Sophia Yan, *Chinese anti-corruption agency warns of 'major problems' in financial sector* (Feb. 5, 2016), https://money.cnn.com/2016/02/05/news/economy/china-financial-sector-corruption-risks/ (discussing "the findings by the ruling Communist Party's Central Commission for Discipline Inspection," and noting that "[m]embers of the Communist Party committee at the financial conglomerate Citic Group were accused of 'talking about business too much while seldom talking about the Party.'")).

[316] *CITIC Group Corporation—Board of Directors and Senior Management*; *Institution Order*, 36 FCC Rcd at 6390, para. 33 (citing *CITIC Group Corporation—Board of Directors and Senior Management*).

[317] *See CITIC Limited Board of Directors*; *CITIC Group Corporation Board of Directors and Senior Management*; *Institution Order*, 36 FCC Rcd at 6390-91, para. 33 (citing *CITIC Limited Board of Directors*). CITIC Limited is a publicly traded entity that is incorporated in Hong Kong and listed on the Hong Kong Stock Exchange. *See* PN/CN June 1, 2020 Response at 10, 12; *id.*, Exh. A. CITIC Limited publicly describes itself as "one of China's largest conglomerates and a constituent of the Hang Seng Index." CITIC Limited 2020 Annual Report at Aiii. According to the Companies, "the only two links of ownership between the ultimate parent, [CITIC Group Corporation], and the Companies that do not represent 100% ownership are (1) the link immediately above CITIC Limited (a public company) which aggregates 58.13% ownership, and (2) the link immediately above CITIC Tel (also a public company) which aggregates 58.12% ownership." PN/CN June 1, 2020 Response at 33.

[318] *CITIC Group Corporation—Board of Directors and Senior Management*; *Institution Order*, 36 FCC Rcd at 6391, para. 33 (citing *CITIC Group Corporation—Board of Directors and Senior Management*).

[319] *CITIC Group Corporation—Board of Directors and Senior Management*; *CITIC Tel—Leadership*; *see CITIC Limited Senior Management*.

Corporation also constitute the senior management of CITIC Limited.[320] One such individual is identified as a leader of the Central Commission for Discipline Inspection of the Communist Party of China and the National Supervisory Commission.[321] Further, based on CITIC Group Corporation's corporate governance information, a "Deputy Party Secretary" is also the "Chairman of the Board of Supervisors."[322]

61. We find that the Chinese government has the ability to influence the Companies through the ties of the corporate leadership of their indirect parent entities with the Chinese Communist Party, as described above. As we stated in the *Institution Order*, "[p]ublicly available information about [the Companies'] indirect parent entities supports the concern raised both by the Executive Branch agencies and the Commission in other proceedings regarding the Chinese government's ability to influence state-owned enterprises,[323] and consequently their indirect subsidiaries, through Chinese Communist Party organizations."[324] The Companies have provided no persuasive argument or evidence to dispel concerns raised by the record evidence demonstrating the significant ties that the corporate leadership of their indirect parent entities have with the Chinese Communist Party and, consequently, the Chinese government.[325] Furthermore, our determination here is consistent with our findings in other proceedings

[320] *CITIC Group Corporation—Board of Directors and Senior Management*; *CITIC Limited Board of Directors*; *CITIC Limited Senior Management*; *Institution Order*, 36 FCC Rcd at 6391, para. 33 (citing *CITIC Group Corporation—Board of Directors and Senior Management*; *CITIC Limited Board of Directors*; *CITIC Limited Senior Management*). One of the individuals identified as a "Party Committee Member" of CITIC Group Corporation is an Executive Director of CITIC Limited. *CITIC Group Corporation—Board of Directors and Senior Management*; *CITIC Limited Board of Directors*; *Institution Order*, 36 FCC Rcd at 6391, para. 33 & n.151 (citing *CITIC Limited Board of Directors*).

[321] *See CITIC Limited Board of Directors* ("currently serves as leader of Discipline Inspection and Supervision Group of CITIC Group Corporation for The Central Commission for Discipline Inspection of the [Communist Party of China] and The National Supervisory Commission"); *CITIC Group Corporation—Board of Directors and Senior Management*; *Institution Order*, 36 FCC Rcd at 6391, para. 33 (citing *CITIC Limited Board of Directors*; *CITIC Group Corporation—Board of Directors and Senior Management*).

[322] *CITIC Group Corporation—Board of Directors and Senior Management*; *see Institution Order*, 36 FCC Rcd at 6391, para. 33 (*CITIC Group Corporation—Board of Directors and Senior Management*). CITIC Group Corporation publicly describes the "mandate of the Board of Supervisors" as "[e]xamining business operations and financial positions of the Group," "[s]upervising the actions taken by Directors and the Management," and "[r]eviewing the Group's Annual Business Plan, Annual Report, the Board of Supervisors' Work Report and proposals on the relevant policies formulated by the Board of Supervisors." *CITIC Group Corporation Corporate Governance and Risk Management*.

[323] *Institution Order*, 36 FCC Rcd at 6389, para. 33 (citing *China Mobile USA Order*, 34 FCC Rcd at 3369-70, para. 18; *China Telecom Americas Institution Order*, 35 FCC Rcd at 15018-20, para. 23).

[324] *Institution Order*, 36 FCC Rcd at 6389-90, para. 33 (citing Office of the U.S. Trade Representative, Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974 at 81, n.446 (2018), https://go.usa.gov/xsmGF (USTR 2018 Section 301 Report) (noting that "[t]he guiding principles" for Chinese government ownership and control are set forth in the Constitution of the People's Republic of China and the Chinese Communist Party Constitution); U.S. Trade Representative, 2020 Report to Congress on China's WTO Compliance at 8 (2021), https://go.usa.gov/xsmGM (stating that "a thorough examination of China's Constitution, relevant directives and pronouncements by China's leadership, legislative and regulatory measures issued by the Chinese government, China's industrial plans and the actions of the Chinese government and the Chinese Communist Party leaves no doubt that the Chinese state maintains a tight grip on virtually all economic activity."); U.S. Trade Representative, 2018 Report to Congress on China's WTO Compliance at 12 (2019), https://go.usa.gov/xsmGe (stating that, "[t]o fulfill these [constitutional] mandates, the government and the Party direct and channel economic actors to meet the state's planning targets")).

[325] *See Institution Order*, 36 FCC Rcd at 6389-91, para. 33.

regarding the influence of the Chinese Communist Party and, consequently, the Chinese government over other Chinese state-owned entities and their U.S. subsidiaries and the threats that the retention of section 214 authority by such subsidiaries pose to the United States.[326] For instance, in the *China Telecom Americas Order on Revocation and Termination*, we stated that national security and law enforcement concerns "stem from the integrated presence and the extent of influence of the Chinese Communist Party, including in military and economic sectors,"[327] and that "[t]he U.S. government has found that the Chinese government exerts influence over state-owned enterprises through the Chinese Communist Party."[328] Further, we acknowledged the Executive Branch agencies' observation that, "[a]ccording to the Chinese government, the [amendments to the Revised Constitution of the Communist Party of China] were made to 'define the status and role of Party organizations in State-owned enterprises.'"[329] As we

[326] *See*, *e.g.*, *China Telecom Americas Order on Revocation and Termination* at *22, para. 59; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 61.

[327] *China Telecom Americas Order on Revocation and Termination* at *22, para. 59 & n.251 (citing Executive Branch CTA Recommendation, Exh. 113 at EB-2379-83, Full text of resolution on amendment to [Communist Party of China] Constitution, State Council of the People's Republic of China, http://english.www.gov.cn/news/top_news/2017/10/24/content_281475919837140.htm (Oct. 24, 2017) (Resolution on the Revised Constitution of the Communist Party of China); *id.*, Exh. 114 at EB-2384-2411, Constitution of the Communist Party of China, Revised and adopted at the 19th National Congress (Oct. 24, 2017), http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf (Revised Constitution of the Communist Party of China)); *see China Unicom Americas Order on Revocation*, FCC 22-9 at para. 61 & n.269. The Revised Constitution of the Communist Party of China states, among other things, that "[t]he Communist Party of China shall uphold its absolute leadership over the People's Liberation Army and other people's armed forces . . . and pursue the Belt and Road Initiative." Revised Constitution of the Communist Party of China at 7-8 ("General Program"); *China Telecom Americas Order on Revocation and Termination* at *22, para. 59, n.251 (citing Executive Branch CTA Recommendation, Exh. 113 at EB-2381, Resolution on the Revised Constitution of the Communist Party of China); *see Worldwide Threat Assessment of the U.S. Intelligence Community: Before the S. Select Comm. On Intelligence*, 116th Cong. at 25 (2019) (statement of Daniel R. Coats, Director of National Intelligence), https://go.usa.gov/xe7ht (2019 ODNI Threat Assessment) ("We assess that China's leaders will try to extend the country's global economic, political, and military reach while using China's military capabilities and overseas infrastructure and energy investments under the Belt and Road Initiative to diminish US influence."). Significantly, the Resolution on the Revised Constitution of the Communist Party of China states that "the Party exercises overall leadership over all areas of endeavor in every part of the country," and "[Party members are obligated] to consciously observe the Party's political discipline and rules." Resolution on the Revised Constitution of the Communist Party of China; *China Telecom Americas Order on Revocation and Termination* at *22, para. 59 (quoting Executive Branch CTA Recommendation to Revoke and Terminate, Exh. 113 at EB-2382, Resolution on the Revised Constitution of the Communist Party of China).

[328] *China Telecom Americas Order on Revocation and Termination* at *22, para. 59; *see China Unicom Americas Order on Revocation*, FCC 22-9 at para. 61. The *China Telecom Americas Order on Revocation and Termination* noted, for example, the assessment of the United States Trade Representative in its 2018 Report on Findings of the Investigation into China's Acts, Policies, and Practices that "[t]he guiding principles for government ownership and control are set forth in the Constitution of the People's Republic of China . . . and the [Chinese Communist Party] Constitution" and that "[t]hrough the [Chinese Communist Party], the Chinese government exercises additional control over [state-owned enterprise] behavior." *See id*. (quoting Executive Branch CTA Recommendation, Exh. 60 at EB-1063, 1066, USTR 2018 Section 301 Report); USTR 2018 Section 301 Report at 81 & n.446, 84. We also noted the analysis in USTR's 2018 Section 301 Report in the *Institution Order*. *See Institution Order*, 36 FCC Rcd at 6390, n.143 (citing USTR 2018 Section 301 Report at 81, n.446 and noting from the Report that "'[t]he guiding principles' for Chinese government ownership and control are set forth in the Constitution of the People's Republic of China and the Chinese Communist Party Constitution").

[329] *See China Telecom Americas Order on Revocation and Termination* at *22, para. 59 (quoting Executive Branch CTA Recommendation at 36 and noting citation to *id.*, Exh. 113 at EB-2382, Resolution on the Revised Constitution of the Communist Party of China); *see id.* at *20, para. 54; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 61; *see supra* note 328; Executive Branch Nov. 16, 2020 Letter at 2 (stating, "[w]e provide our views regarding whether the Companies are subject to the exploitation, influence, and control of the Chinese government, (continued….)

stated in the *Institution Order*, according to Article 33 of the Revised Constitution of the Communist Party of China, "'[p]rimary-level Party organizations shall guarantee and oversee the implementation of the principles and policies of the Party and the state within their own enterprise and shall support the board of shareholders, board of directors, board of supervisors, and manager (or factory director) in exercising their functions and powers in accordance with the law.'"[330] We find that there is no evidence in the record to show that the Companies have measures in place to counter the strong presence of the Chinese Communist Party within their indirect parent entities and the ability of the Chinese Communist Party to influence and control the operations, corporate policies, decision-making, and other activities of the indirect parent entities, and consequently, the Companies, to further the goals and priorities of the Chinese Communist Party and the Chinese government.

62. The Companies also argue, "[w]hile the *Orders* have focused entirely on state ownership of CITIC Group Corporation, [CITIC Tel] . . . is a publicly-listed company on the Hong Kong Stock Exchange, with a diversified shareholder group" and "[t]o comply with the Listing Rules of the Hong Kong Stock Exchange, CITIC Tel provides transparency in its financial operations comparable to that of companies listed on U.S. and international stock exchanges, making its governance and financial reports publicly available."[331] The Companies contend that "any material decisions—major transactions, substantial disposals of assets or acquisitions, etc.—of CITIC Tel must be taken through meetings of the

(Continued from previous page)
and the national security and law enforcement risks associated with such exploitation, influence, and control. These risks will come as no surprise to the FCC, as the same risks were applicable and were identified in detail in the recommendation submitted to the FCC concerning China Telecom Americas Corporation's ('China Telecom') international Section 214 authorizations.").

[330] *Institution Order*, 36 FCC Rcd at 6389, n.142 (quoting Revised Constitution of the Communist Party of China, Article 33); Revised Constitution of the Communist Party of China, Article 33. We also recognized that under Article 32 of the Revised Constitution of the Communist Party of China, "[p]rimary-level Party organizations play a key role for the Party in the basic units of social organization" and their "main tasks" include "to encourage Party members and the people to consciously resist unacceptable practices and resolutely fight against all violations of Party discipline or state law." Revised Constitution of the Communist Party of China, Article 32; *Institution Order*, 36 FCC Rcd at 6389, n.142 (quoting Revised Constitution of the Communist Party of China, Article 32). We further stated that Article 33 of the Revised Constitution of the Communist Party of China states, among other things, that "[t]he leading Party members groups or Party committees of state-owned enterprises shall play a leadership role, set the right direction, keep in mind the big picture, ensure the implementation of Party policies and principles, and discuss and decide on major issues of their enterprise in accordance with regulations." Revised Constitution of the Communist Party of China, Article 33; *Institution Order*, 36 FCC Rcd at 6389, n.142 (quoting Revised Constitution of the Communist Party of China, Article 33). Moreover, as we stated in the *Institution Order*, Article 19 of the Company Law of the People's Republic of China (2018 Amendment) states that "[t]he Chinese Communist Party may, according to the Constitution of the Chinese Communist Party, establish its branches in companies to carry out activities of the Chinese Communist Party," and that "[t]he company shall provide necessary conditions to facilitate the activities of the Party." Lawinfochina, Company Law of the People's Republic of China (2018 Amendment) at Article 19, http://lawinfochina.com/display.aspx?id=e797dd968c30e172bdfb&lib=law (last visited Mar. 16, 2022) (2018 Company Law); *Institution Order*, 36 FCC Rcd at 6389, n.142 (quoting 2018 Company Law, Article 19); *see infra* para. 72.

[331] PN/CN *Ex Parte* Letter at 2; *see* PN/CN June 1, 2020 Response at 12 ("[T]he two public company entities in the ownership structure, CITIC Limited and CITIC Tel, are publicly traded companies listed on the Hong Kong Stock Exchange . . . and those companies are subject to the regulatory and disclosure requirements of the Hong Kong Listing Rules and other applicable regulations"). The Companies argue, "CITIC Tel and its Board of Directors must observe its Articles of Association and the requirements of the Listing Rules in making any decisions regarding its own operations, or any decisions that might impact the Companies." PN/CN *Ex Parte* Letter at 2 (citing https://www.hkex.com.hk/Listing/Listed-Issuers/Practices-and-Procedures-for-Handling-Listing-related-Matters?sc_lang=en) (referring to this information as "guides . . . .").

company's shareholders."[332] That CITIC Tel, an indirect parent of the Companies, may be subject to the Hong Kong Stock Exchange Listing Rules, even assuming full compliance with such rules, does not assuage our concerns.[333] Although the Companies argue, with respect to CITIC Tel, that there is "participation of significant levels of public, international ownership"[334] and it is "subject to external transparency and accountability requirements,"[335] they state nevertheless that CITIC Group Corporation is "the actual controlling party" of its subsidiaries, which include CITIC Tel and the Companies.[336] The Companies offer no persuasive argument or evidence that CITIC Group Corporation, the ultimate controlling parent, is not significantly influenced by the Chinese Communist Party and the Chinese government and cannot, as a consequence, influence and control the operations and corporate policies of its subsidiaries, notwithstanding any "external transparency and accountability requirements"[337] that may apply to the publicly-traded subsidiaries, CITIC Tel and CITIC Limited. Moreover, based on information made publicly available by CITIC Tel, CITIC Tel similarly states that CITIC Group Corporation is "the controlling shareholder of the Group."[338] We thus find unpersuasive any suggestion by the Companies that other shareholders of CITIC Tel can provide a balance in perspective or influence to that of CITIC Group Corporation, and ultimately, the influence and control of the Chinese government. In the absence of record evidence showing otherwise, the existence of the Hong Kong Stock Exchange Listing Rules and their applicability to CITIC Tel do not convince us that the Chinese government is unable to exert its influence and control over the Companies through CITIC Group Corporation or its subsidiaries, including CITIC Tel.

63. *Chinese Laws and the Companies' Ownership May Force the Companies to Carry Out Certain Activities that are Harmful to U.S. Interests.* We agree with the Executive Branch agencies' assessment and find that "[t]he Chinese government's majority ownership and control of the Companies through [CITIC Group Corporation], combined with Chinese intelligence and cybersecurity laws, raise significant concerns that the Companies will be forced to comply with Chinese government requests, including requests for communications intercepts, without the ability to challenge such requests."[339] This

[332] PN/CN *Ex Parte* Letter at 2 (citing "Chapter 14, Notifiable Transactions, HKEX Listing Rules, https://en-rules.hkex.com.hk/rulebook/chapter-14-notifiable-transactions").

[333] *See id.*

[334] *Id.*

[335] *Id*.

[336] PN/CN June 1, 2020 Response at 6-7. In explaining that "[n]o material change of ultimate ownership was effected by" the 2014 transaction concerning which the Companies failed to file timely *pro forma* notifications in compliance with the Commission's rules, the Companies state that, "[a]fter the transaction, CITIC Group Corporation continued to *control* over 50% of CITIC Limited, and ultimately to *control* over 50% of Pacific Networks and ComNet . . . As a result, the 2014 ownership change was one which did not result in a change in the *actual controlling party* and is therefore considered non-substantial or *pro forma*." *Id.* (emphasis added) (citing 47 CFR § 63.24(d)); *see infra* para. 135; *see id.* at 10 (describing "the ownership by Richtone Enterprises Inc., Ease Action Investments Corp., Perfect New Holdings Limited and Silver Log Holdings Ltd., *each of which is an indirect controlled subsidiary of CITIC Group Corporation*, of an aggregate of 58.12% of the equity of [CITIC Tel], a publicly-traded company the stock of which is listed on the Hong Kong Stock Exchange") (emphasis added).

[337] *See* PN/CN *Ex Parte* Letter at 2.

[338] CITIC Tel 2021 Interim Report at 9; *id.* ("About Us") (defining "Group" as "CITIC Telecom International Holdings Limited (the 'Company', and together with its subsidiaries the 'Group'"); CITIC Tel 2020 Annual Report at 72 (identifying CITIC Group Corporation as "the ultimate controlling shareholder of the Company"); *id.* at 208 ("As at 31 December 2020, the directors consider the immediate parent and *the ultimate controlling party* of the Group to be Ease Action Investments Corp., which is incorporated in the British Virgin Islands, *and CITIC Group Corporation, which is a wholly state-owned company in the [People's Republic of China], respectively*.") (emphasis added).

[339] Executive Branch Nov. 16, 2020 Letter at 6.

determination is based on the Chinese government's influence and control over the Companies and their parent entities through, among other things, the ties of the Companies' parent entities with the Chinese Communist Party and the requirements of Chinese laws that have been enacted in recent years.[340] We find that the combination of these laws—the 2017 Cybersecurity Law,[341] its implementing regulation (2018 Cybersecurity Regulation),[342] 2017 National Intelligence Law,[343] and the 2019 Cryptography Law[344]—raises substantial and serious national security and law enforcement risks. Specifically, as indicated by the Executive Branch agencies, we find that the 2017 Cybersecurity Law and the 2017 National Intelligence Law "impose affirmative legal responsibilities on Chinese and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for Beijing's intelligence gathering activities."[345] The Executive Branch agencies add that the provisions of China's 2019 Cryptography Law "impose requirements that will expose commercial encryption used within China to testing and certification by the Chinese government, potentially facilitating those same intelligence activities."[346]

64. We conclude that the 2017 Cybersecurity Law and the 2018 Cybersecurity Regulation give the Chinese government authority over the Companies' ultimate parent entity and the Companies are therefore vulnerable to these laws.[347] The Executive Branch agencies assert that the Companies' ultimate parent, CITIC Group Corporation, "as a state-owned entity, is subject to these Chinese cyber and national security laws."[348] The Companies do not dispute this, but contend that the "2017 Cybersecurity Law states that it is 'applicable to the construction, operation, maintenance, and use of networks, as well as to

[340] *Institution Order*, 36 FCC Rcd at 6392-93, para. 35; Executive Branch Nov. 16, 2020 Letter at 6-8.

[341] *Institution Order*, 36 FCC Rcd at 6383-84, 6394-95, paras. 24, 39; Executive Branch Nov. 16, 2020 Letter at 6-8; Executive Branch June 4, 2021 Reply at 2-3; *China Telecom Americas Order on Revocation and Termination* at *22, para. 60; *China Unicom Americas Order on Revocation*, FCC 22-9 at paras. 64-65, 70.

[342] *Institution Order*, 36 FCC Rcd at 6394-95, para. 39; Executive Branch Nov. 16, 2021 Letter at 6-8 (citing *China: New Regulation on Policy Cybersecurity Supervision and Inspection Powers Issued*, Library of Congress (Nov. 13, 2018), https://www.loc.gov/law/foreign-news/article/china-new-regulation-on-police-cybersecurity-supervision-and-inspection-powers-issued/; *China's New Cybersecurity Measures Allow State Policy to Remotely Access Company Systems*, Recorded Future Blog (Feb. 8, 2019), https://www.recordedfuture.com/china-cybersecurity-measures/ (*China's New Cybersecurity Measures*); Executive Branch June 4, 2021 Reply at 2-3; *China Telecom Americas Order on Revocation and Termination* at *22, para. 60; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 65; *see Regulation on Internet Security Supervision and Inspection by Public Security Organs*, http://www.gov.cn/zhengce/zhengceku/2018-12/31/content_5428637.htm (last visited Mar. 16, 2022)); *see* Lawinfochina, Provisions on Internet Security Supervision and Inspection by Public Security Organs (Translation), https://www.lawinfochina.com/display.aspx?id=f37b0d2a40065436bdfb&lib=law (last visited Mar. 16, 2022).

[343] *Institution Order*, 36 FCC Rcd at 6383-84, 6392-94, paras. 24, 35-37; Executive Branch Nov. 16, 2020 Letter at 6-8; Executive Branch June 4, 2021 Reply at 2-3; *China Telecom Americas Order on Revocation and Termination* at *22, 23, paras. 60, 63; *China Unicom Americas Order on Revocation*, FCC 22-9 at paras. 64-65, 70.

[344] *Institution Order*, 36 FCC Rcd at 6383-84, 6394, paras. 24, 39; Executive Branch Nov. 16, 2020 Letter at 6-8; Executive Branch June 4, 2021 Reply at 2-3; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 71.

[345] *See* Executive Branch Nov. 16, 2020 Letter at 6 (citing Statement of Deputy Assistant Attorney General Adam S. Hickey, National Security Division, U.S. Department of Justice); *Institution Order*, 36 FCC Rcd at 6392-95, paras. 35-39.

[346] *See* Executive Branch Nov. 16, 2020 Letter at 6 (citing Statement of Deputy Assistant Attorney General Adam S. Hickey); *Institution Order*, 36 FCC Rcd at 6394, para. 39 (quoting Executive Branch Nov. 16, 2020 Letter at 6).

[347] *Institution Order*, 36 FCC Rcd at 6394-95, para. 39; Executive Branch Nov. 16, 2020 Letter at 6-8; Executive Branch June 4, 2021 Reply at 2-3; *see China Telecom Americas Order on Revocation and Termination* at *22, 23, paras. 60, 63; *China Unicom Americas Order on Revocation*, FCC 22-9 at paras. 64-65.

[348] Executive Branch Nov. 16, 2020 Letter at 8.

cybersecurity supervision and management within the mainland territory of the People's Republic of China'" and therefore "[t]he Companies' network operations in the U.S. would not be subject to the reach of the 2017 Cybersecurity Law."[349] We find, as indicated by the Executive Branch agencies, however, that the 2017 Cybersecurity Law "requires extensive cooperation by telecom and network operators" with the Chinese government.[350] The Executive Branch agencies state that the 2017 Cybersecurity Law and the 2018 Cybersecurity Regulation "impose more specific obligations for telecommunications systems operators, even if they are not state owned,"[351] and the "vague definition" of network operators[352] "ensnares both foreign and Chinese network operators that own or manage a network or provide online services anywhere within China."[353] Further, the Executive Branch agencies explain that the 2018 Cybersecurity Regulation "authorizes the Ministry of Public Security to conduct on-site and remote inspections of any company with five or more networked computers, to copy user information, log security response plans during on-site inspections, and check for vulnerabilities."[354] In addition, "[f]or remote inspections, the Ministry of Public Security would be permitted to use certain cybersecurity service agencies."[355]

[349] PN/CN April 28, 2021 Reply at 12 (citing 2017 Cybersecurity Law, Article 2).

[350] Executive Branch Nov. 16, 2020 Letter at 7; *see China Telecom Americas Order on Revocation and Termination* at *22, para. 60 & n.265 (quoting Executive Branch CTA Recommendation at 38-39); *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 67 & n.308. Further, Article 35 of the 2017 Cybersecurity Law states that "[c]ritical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council." 2017 Cybersecurity Law, Article 35; *see China Telecom Americas Order on Revocation and Termination* at *22, para. 60 (quoting Executive Branch CTA Recommendation, Exh. 51 at EB-876, 2017 Cybersecurity Law, Article 35); *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 67 & n.308 (quoting 2017 Cybersecurity Law, Article 35). Additionally, Article 8 of the 2017 Cybersecurity Law states that "[t]he State Council departments for telecommunications, public security, and other relevant organs, are responsible for cybersecurity protection, supervision, and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law and relevant laws and administrative regulations." 2017 Cybersecurity Law, Article 8; *see China Telecom Americas Order on Revocation and Termination* at *22, para. 60, n.265 (quoting Executive Branch CTA Recommendation, Exh. 51 at EB-869, 2017 Cybersecurity Law, Article 8); *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 67 & n.308 (quoting 2017 Cybersecurity Law, Article 8).

[351] Executive Branch Nov. 16, 2020 Letter at 7.

[352] *Id*. (stating, "'[n]etwork operators' are broadly defined as 'network owners, network managers, and network service providers'") (citing 2017 Cybersecurity Law, Article 76(3)); *see* 2017 Cybersecurity Law, Article 76(3) (providing definition of "Network operators" as "network owners, managers, and network service providers").

[353] Executive Branch Nov. 16, 2020 Letter at 7 (citing 2017 Cybersecurity Law, Article 2; Jones Day, White Paper: Implementing China's Cybersecurity Law (Aug. 2017), https://www.jonesday.com/en/insights/2017/08/implementing-chinas-cybersecurity-law). The Executive Branch agencies state, for example, that Article 28 of the 2017 Cybersecurity Law states, "[n]etwork operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law." *See id.* (quoting 2017 Cybersecurity Law, Article 28); 2017 Cybersecurity Law, Article 28. Additionally, Article 49 of the 2017 Cybersecurity Law states that "[n]etwork operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law." 2017 Cybersecurity Law, Article 49; Executive Branch Nov. 16, 2020 Letter at 7 (quoting 2017 Cybersecurity Law, Article 49); *see China Telecom Americas Order on Revocation and Termination* at *22, para. 60 (quoting Executive Branch CTA Recommendation, Exh. 51 at EB-880, 2017 Cybersecurity Law, Article 49); *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 67 (quoting 2017 Cybersecurity Law, Article 49).

[354] Executive Branch Nov. 16, 2020 Letter at 7-8 (citing *China's New Cybersecurity Measures*)).

[355] *Id*. at 8.

65. Furthermore, we find that the record raises significant concerns about the impact of the 2017 Cybersecurity Law and 2018 Cybersecurity Regulation on the Companies' operations, particularly in light of the Executive Branch agencies' argument that "the Chinese government uses its firms and companies as extensions of its apparatus" and "[t]hose concerns are particularly acute with respect to Chinese state-owned enterprises ('SOE') and their subsidiaries, because the Chinese government is able to exercise direct control over those entities."[356] We also believe that the Companies are vulnerable to Chinese government requests based on the requirements of the 2017 Cybersecurity Law and the 2018 Cybersecurity Regulation. The 2017 Cybersecurity Law requires, among other things, that "[n]etwork operators" shall "provide technical support and assistance to public security organs and national security organs"[357] and "cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections."[358] As discussed above, the record shows how integrated ComNet's and Pacific Networks' operations—{[ ]}—are with that of their indirect parent entity, CITIC Tel, and its subsidiaries, {[ ]} and how closely ComNet and Pacific Networks coordinate with these entities.[359]

66. Significantly, the Companies disclose that they are not solely responsible for protecting and governing access to ComNet's Wholesale IDD records {[ ]}[360] Furthermore, based on the record, {[

[356] *Id*. at 6.

[357] 2017 Cybersecurity Law, Article 28; Executive Branch Nov. 16, 2020 Letter at 7 (quoting 2017 Cybersecurity Law, Article 28).

[358] 2017 Cybersecurity Law, Article 49; Executive Branch Nov. 16, 2020 Letter at 7 (quoting 2017 Cybersecurity Law, Article 49).

[359] *See supra* para. 53.

[360] PN/CN April 28, 2021 Reply at 47-50, 72.

[361] *Id*. at 47-50; *see supra* para. 53.

[362] PN/CN April 28, 2021 Reply at 59; *see supra* para. 53.

[363] PN/CN April 28, 2021 Reply at 72; *id.*, Business Confidential Exh. J at J-2-J-3.

[364] *Id*. at 47-50, 72; *id.*, Business Confidential Exh. J at J-2-J-3.

[365] *Id*. at 47-50; *see supra* para. 53.

[366] {[

(continued….)

]}[367] The Companies have offered no persuasive argument that the Chinese government, through its direct ownership and control of the Companies' ultimate parent entity, could not influence or control subsidiaries of a state-owned entity, such as the Companies, CITIC Tel, {[ ]} to take action in furtherance of China's national intelligence goals based on these laws.[368]

67. The Companies state that, "[a]t no time have any officials of the government of the People's Republic of China or of the Chinese Communist Party directed or requested that Pacific Networks or ComNet take or refrain from taking any particular action."[369] Even if we were to accept the Companies' claims as true, the Companies simply fail to provide record evidence that they could at any time overcome any directive, including through their parent entities, to cooperate with Chinese government requests under these laws. Our concerns are heightened given the Executive Branch agencies' statement that "[b]oth the 2017 Cybersecurity Law and [2018 Cybersecurity Regulation] provide little, if any, detail about the available legal procedures or judicial oversight to challenge any Chinese government requests."[370]

68. Additionally, we find that the 2017 National Intelligence Law raises concerns about the Companies' vulnerability to exploitation, influence, and control by the Chinese government. Our determinations here are consistent with the Commission's prior findings that the 2017 National Intelligence Law requires that "[a]ll organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of."[371] We agree with the Executive Branch agencies' assessment that "[t]he 2017

(Continued from previous page)

]}

[367] *See* Executive Branch Nov. 16, 2020 Letter at 6.

[368] *See, e.g.*, 2018 Cybersecurity Law, Article 28 ("Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."); *see supra* note 353 (addressing Article 28 of the 2018 Cybersecurity Law).

[369] PN/CN April 28, 2021 Reply, Declaration of Li Ying (Linda) Peng; PN/CN June 1, 2020 Response, Declaration of Li Ying (Linda) Peng.

[370] Executive Branch Nov. 16, 2020 Letter at 8.

[371] 2017 National Intelligence Law, Article 7; *see China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17; *Huawei Designation Order*, 35 FCC Rcd at 14440, para. 16; *China Telecom Americas Order on Revocation and Termination* at *23, para. 63; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 65 & n.293; *Institution Order*, 36 FCC Rcd at 6383-84, para. 24. The Executive Branch agencies note, in particular, that in the *China Mobile USA Order*, the Commission stated, "Article 7 of the 2017 National Intelligence Law provides 'an

(continued….)

Intelligence Law provides Chinese government's intelligence services with greater powers to compel Chinese citizens and organizations 'to cooperate, assist, and support Chinese intelligence efforts *wherever they are in the world*.'"[372] As we stated in the *Institution Order*, the former U.S. National Security Advisor has warned that under Article 7 of China's National Intelligence Law, "all Chinese companies must collaborate in gathering intelligence."[373] Moreover, as we stated in the *Institution Order*, "'the Chinese government is highly centralized and exercises strong control over commercial entities, permitting the government, including state intelligence agencies, to demand that private communications sector entities cooperate with any governmental requests, which could involve revealing customer information, including network traffic information.'"[374] Therefore, we find unpersuasive the Companies' assertion that, "[a]s U.S. companies, the Companies are not permitted under U.S. law to support another country's intelligence gathering activities, thus the National Intelligence Law could not be used to direct such efforts, as it would be in contradiction of the law itself."[375] The Companies offer no persuasive argument or evidence to dispel the significant concerns raised by the record that the Chinese government could require the Companies, as subsidiaries of a Chinese state-owned entity, to support the Chinese government's intelligence efforts through the influence and control that the Chinese government and the Companies' parent entities can exert on the Companies.

(Continued from previous page)
organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows.' Article 14 permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation. Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, including communications equipment." Executive Branch Nov. 16, 2020 Letter at 6-7 (quoting *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17); *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17 (citing The National People's Congress of the People's Republic of China, National Intelligence Law of the People's Republic, http://www npc.gov.cn/npc/xinwen/2017-06/27/content 2024529 htm (last visited April 16, 2019); pkulaw.cn, National Intelligence Law of the People's Republic of China (2018 Amendment), http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law (last visited Apr. 16, 2019) (English-language translation)).

[372] Executive Branch Nov. 16, 2020 Letter at 6 (quoting *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17 and citing Carolina Dackö and Lucas Jonsson, Applicability of National Intelligence Law to Chinese and non-Chinese Entities, Mannheimer Swartling (Jan. 2019), https://www.mannheimerswartling.se/app/uploads/2021/04/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf; National Intelligence Law of the People's Republic, National People's Congress (last visited Mar. 24, 2020), https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (Google's cache of http://www.npc.gov.cn/npc/xinwen/201706/27/content_2024529 htm)) (emphasis added); *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17 (emphasis added).

[373] *See Institution Order*, 36 FCC Rcd at 6384, para. 24 (citing *What China Wants* at 70, 71, 72-73); *see* Executive Branch Nov. 16, 2020 Letter at 6-7; *China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at *23, para. 63 (citing *What China Wants* at 70, 71, 72-73); *China Telecom Americas Institution Order*, 35 FCC Rcd at 15018, para. 22 (citing *What China Wants* at 70, 71, 72-73). Additionally, as noted in the *Institution Order*, the Office of the Secretary of Defense stated in its 2019 report on Military and Security Developments Involving the People's Republic of China that "[t]he 2017 *National Intelligence Law* requires Chinese companies . . . to support, provide assistance, and cooperate in China's national intelligence work, wherever they operate." Office of the Secretary of Defense Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019 at 101 (May 2, 2019), https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf (2019 China Military and Security Developments Report); *Institution Order*, 36 FCC Rcd at 6392, n.164 (citing *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17 and quoting 2019 China Military and Security Developments Report at 101)); *China Telecom Americas Order on Revocation and Termination* at *23, para. 63 (quoting Executive Branch CTA Recommendation Exh. 115 at EB-2524, 2019 China Military and Security Developments Report at 101).

[374] *Institution Order*, 36 FCC Rcd at 6392, para. 35 (quoting *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, para. 46 and citing *What China Wants* at 69-74).

[375] PN/CN April 28, 2021 Reply at 11.

69. The Commission has rejected arguments that the 2017 National Intelligence Law does not apply to U.S. subsidiaries of Chinese entities, and we reject them again here.[376] In the 2020 *Huawei Designation Order*, the Commission "reject[ed] Huawei's claim that the National Intelligence Law does not apply to Huawei's U.S. subsidiary because . . . Chinese law does not have extraterritorial effect, and Huawei has never been asked by Chinese governmental entities to conduct espionage on behalf of the Chinese government."[377] The Commission considered "the broad sweep of Article 11 of the National Intelligence Law, which authorizes Chinese intelligence agencies to act abroad, and the Executive Branch's interpretation of the Chinese legal regime, which holds that Chinese law imposes affirmative legal responsibilities on both Chinese and foreign citizens, companies, and organizations operating in China to assist with Chinese intelligence-gathering activities."[378]

[376] *Institution Order*, 36 FCC Rcd at 6393-94, para. 37; *id.* at 6393, para. 36 (citing PN/CN June 1, 2020 Response at 26); *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11442, para. 49; *Huawei Designation Order*, 35 FCC Rcd at 14441-42, para. 20. In the *Protecting Against National Security Threats Order*, the Commission stated that "we are not persuaded to excuse these affiliates from the scope of our prohibition. One expert has noted that the nature of the Chinese system 'recognizes no limits to government power.' Irrespective of their physical location, these affiliates still remain subject to Chinese law." *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11442, para. 49; *Institution Order*, 36 FCC Rcd at 6393, para. 37 (quoting *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11442, para. 49). The Commission further stated, "[t]he fact that [Huawei Technologies Company's (Huawei)] subsidiaries act outside of China does not mean that their parent company lacks influence over their operations and decisions given the strong influence that Huawei's parent companies and the Chinese government can exert over their affiliates." *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11446, para. 56; *Institution Order*, 36 FCC Rcd at 6393, para. 37 (quoting *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11442, para. 56). In their response to the *Institution Order*, the Companies contend that the *Institution Order* "does not cite to any evidence that the Chinese laws have actually been used to compromise the Companies in any way" and "relies on hypothetical scenarios based on the possibility that the laws could be interpreted in such a way as to impact the U.S.-based entities." PN/CN April 28, 2021 Reply at 13. The Companies argue that "the plain language" of these Chinese laws "rais[es] a material question as to the extent of compulsion under the laws as applied to the Companies' operations." *Id.* at 11. The Companies state that "[t]he conclusions are not based on fact, or an analysis specific to the Companies' operations" and "[t]he Companies have repeatedly stated that they have not been asked by the Chinese government to do anything in contradiction of U.S. law and do not believe that they could be asked to do so." *Id.* at 13.

[377] *Huawei Designation Order*, 35 FCC Rcd at 14441, para. 20 (citation omitted); *Institution Order*, 36 FCC Rcd at 6393, para. 37 (quoting *Huawei Designation Order*, 35 FCC Rcd at 14441, para. 20).

[378] *Huawei Designation Order*, 35 FCC Rcd at 14441-42, para. 20 (citing *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs–Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604, 6614, para. 23 (PSHSB 2020) (*PSHSB 2020 Huawei Order*); NTIA Huawei June 9, 2020 Letter at 5); *Institution Order*, 36 FCC Rcd at 6393, para. 37 (quoting *Huawei Designation Order*, 35 FCC Rcd at 14441-42, para. 20). Article 11 of the 2017 National Intelligence Law states, "[n]ational intelligence work institutions shall lawfully collect and handle intelligence related to foreign institutions, organizations or individuals carrying out, directing or funding foreign or domestic institutions, organizations, or individuals colluding to carry out, conduct endangering the national security and interests of the People's Republic of China; so as to provide intelligence references and bases for preventing, stopping, and punishing the above conduct." China Law Translate, 2017 National Intelligence Law, Article 11. Moreover, in the *Huawei Designation Order*, the Commission found that "employees of Huawei's U.S. subsidiaries are susceptible to coercion by Huawei China, and by extension Chinese intelligence." *Huawei Designation Order*, 35 FCC Rcd at 14442, para. 21; *Institution Order*, 36 FCC Rcd at 6393-94, para. 37 (quoting *Huawei Designation Order*, 35 FCC Rcd at 14442, para. 21). We believe a similar rationale applies here, notwithstanding the Companies' claim that their U.S. employees would expose themselves to great personal risk in violating U.S. law or data privacy policies: The Companies or their affiliates could direct employees to take unlawful actions, and an employee may not realize the action violates a law or data privacy policy. Even where an employee or official knowingly takes wrongful action, the risk of legal liability depends on whether the misconduct is likely to be detected. *See* PN/CN June 1, 2020 Response at 26 (arguing the *Order to Show Cause* "does not explain the basis for believing that this law would apply equally to relatively small, independently-operated, U.S. domiciled companies that are not wholly-owned by the Chinese government, when the (continued….)

70. Further, we find unpersuasive the Companies' suggestion that the Chinese government construes or would construe "lawful rights and interests of individuals and organizations" in favor of U.S. law to whatever extent the 2017 National Intelligence Law and any actions directed or undertaken pursuant to that law conflicts with U.S. law.[379] Given the record evidence and our findings in other proceedings, we agree with the Executive Branch agencies that "[t]he Companies' argument . . . rests on the dubious proposition that the Chinese government will prioritize U.S. laws over its own laws."[380] The Executive Branch agencies further state that the Companies' argument "rests on the entirely faulty assumption that the Chinese government will respect the rule of law to begin with."[381] The Companies contend that such an assessment is contradictory, arguing, "the entire case is based on a contradiction: the NTIA Letter wants to say that changes to Chinese laws increased the risk and now require action against the Companies, but then wants to ignore criticisms of its analysis by saying the Chinese government can do whatever it wants anyway."[382] We find no such contradiction. The Executive Branch agencies' assessment of the risks associated with the 2017 National Intelligence Law, and the other Chinese laws, is

(Continued from previous page)
implementation of any such request would expose U.S. personnel of the Companies to considerable risk of prosecution"); *id.*, Declaration of Li Ying (Linda) Peng; PN/CN April 28, 2021 Reply, Declaration of Li Ying (Linda) Peng; PN/CN June 1, 2020 Response at 25-26 (stating, "[t]he totality of ComNet's employees are subject to United States laws—either by virtue of full citizenship, their status as a green card holder or in one case an H1-B visa holder" and "[a]ny employee modifying operations at the direction of foreign influence would expose himself or herself to tremendous personal legal risk"). As we stated above, the Companies offer no persuasive arguments to refute the concerns that the Chinese government has influence and control over the Companies through, for instance, the ties of their parent entities with the Chinese Communist Party and the Chinese government, or that the Chinese government could also directly influence the Companies to take certain actions. *See supra* paras. 58--69.

[379] PN/CN April 28, 2021 Reply at 11 (arguing, "[t]he National Intelligence Law specifies that its restrictions 'shall be conducted in accordance with law . . . and shall preserve the lawful rights and interests of individuals and organizations'" and that "[a]s U.S. companies, the Companies are not permitted under U.S. law to support another country's intelligence gathering activities, thus the National Intelligence Law could not be used to direct such efforts, as it would be in contradiction of the law itself") (emphasis omitted); *see supra* para. 68-69. The full text of Article 8 of the 2017 National Intelligence Law states, "[n]ational intelligence efforts shall be conducted in accordance with law, shall respect and protect human rights, and shall preserve the lawful rights and interests of individuals and organizations." 2017 National Intelligence Law, Article 8.

[380] Executive Branch June 4, 2021 Reply at 2-3; Executive Branch Nov. 16, 2020 Letter at 2-8 (discussing changed national security environment and national security and law enforcement risks associated with Chinese cyber and national security laws); *see supra* paras. 68-69; *Huawei Designation Order*, 35 FCC Rcd at 14441-42, para. 20 (citing *PSHSB 2020 Huawei Order*, 35 FCC Rcd at 6614, para. 3; NTIA Huawei June 9, 2020 Letter at 5); *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17. In this regard, we reject the Companies' claim that there is a material question of fact as to whether they "ever have or ever would violate the law of the United States or their own data privacy policies . . . by misusing access to such [personally identifiable information and CPNI] data." PN/CN April 28, 2021 Reply at 39. As set forth above, we conclude that that the Companies are vulnerable to exploitation, influence, and control by the Chinese government, and we need not wait until national security risks have been exploited before we act to prevent such threats.

[381] Executive Branch June 4, 2021 Reply at 2-3.

[382] PN/CN June 28, 2021 Reply at 4; *id.* (arguing, "[i]f this is true, then the 'change' in law changed nothing. The NTIA Letter thus makes clear that the Monitoring Agencies have manufactured a 'change in circumstances' that does not actually exist in order to justify voiding the 2009 Letter of Assurance and avoiding any engagement in discussion of how real, identified security risks might be mitigated."). We note, among other things, that this assertion by the Companies neglects to address, let alone refute, the overwhelming evidence in the record that demonstrates that the national security environment has changed significantly since the Commission authorized Pacific Networks and ComNet to provide telecommunications services in the United States and that, given the changed national security environment with respect to China, the Companies' ownership and control by the Chinese government raise significant and substantial national security and law enforcement risks. *See supra* para. 2, 14; *see infra* para. 77; *Institution Order*, 36 FCC Rcd at 6397-98, paras. 42-43.

supported by the record evidence documenting the heightened national security and law enforcement risks posed by the Chinese government's actions in the current national security environment.[383]

71. With respect to the 2019 Cryptography Law, we are unpersuaded by the Companies' suggestion that this law cannot reach the Companies, particularly given the record evidence that shows that {[

]}[384] and "coordinate[]" with the Companies to manage access to these records,[385] and that these entities have an integrated role in the Companies' provisioning of services.[386] We agree with the Executive Branch agencies' statement that provisions "contained in the 2019 Cryptography Law, impose requirements that will expose commercial encryption used within China to testing and certification by the Chinese government, potentially facilitating" the Chinese government's intelligence gathering activities.[387] Specifically, according to a Deputy Assistant Attorney General for the U.S. Department of Justice, National Security Division, Article 26 of the 2019 Cryptography Law "requires any '[c]ommercial cryptography products that involve national security, the national welfare and the people's livelihood, or the societal public interest' to be tested and certified by Chinese government authorities, pursuant to the relevant provisions of the 2017 Cybersecurity Law."[388] In

[383] *See supra* paras. 2, 14; *see infra* para. 77; Executive Branch Nov. 16, 2020 Letter at 2-8 (discussing changed circumstances in the national security environment and national security and law enforcement risks associated with Chinese cyber and national security laws); Executive Branch CTA Recommendation at 2-7. Moreover, the Companies offer no rebuttal to the Executive Branch agencies' concerns relating to the findings of U.S. government agencies, such as the U.S. Department of State's 2020 Country Report on China that is noted by the Executive Branch agencies, that "the Chinese government has little regard for the rights and interests of individuals and organizations, including: 'politically motivated reprisal against individuals outside the country; the lack of an independent judiciary and Communist Party control over the judicial and legal system; arbitrary interference with privacy; pervasive and intrusive technical surveillance and monitoring . . . .'" Executive Branch June 4, 2021 Reply at 3 (quoting U.S. Department of State, Bureau of Democracy, Human Rights and Labor, 2020 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet), , "Executive Summary" (Mar. 30, 2021), https://go.usa.gov/xttQh (2020 Country Report on China)); U.S. Department of State, Bureau of Democracy, Human Rights and Labor, *2020 Country Reports on Human Rights Practices* (Mar. 30, 2021), https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/ (identifying date of 2020 Country Reports on Human Rights Practices and providing link to 2020 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)). The 2020 Country Report on China further states, among other things, "[a]lthough officials faced criminal penalties for corruption, the government and the [Chinese Communist Party] did not implement the law consistently or transparently . . . Court judgments often could not be enforced against powerful special entities, including government departments, state-owned enterprises, military personnel, and some members of the [Chinese Communist Party]." 2020 Country Report on China at 53.

[384] PN/CN April 28, 2021 at 47-51, 72; *id.*, Business Confidential Exh. J at J-2-J-3.

[385] *Id*. at 47-50.

[386] *Id*. at 47-50, 72; *see id.*, Business Confidential Exh. J.

[387] Executive Branch Nov. 16, 2020 Letter at 6 (quoting Statement of Deputy Assistant Attorney General Adam S. Hickey at 6); Statement of Deputy Assistant Attorney General Adam S. Hickey at 6.

[388] Statement of Deputy Assistant Attorney General Adam S. Hickey at 7 (citing U.S.-China Economic and Security Review Commission, Economics and Trade Bulletin at 13 (Nov. 5, 2019), https://go.usa.gov/xttUr (USCC November 5, 2019 Economics and Trade Bulletin); 2019 Cryptography Law). Specifically, Article 26 of the 2019 Cryptography Law states, among other things, "[c]ommercial cryptography products that involve national security, the national welfare and the people's livelihood, or the societal public interest, shall be lawfully entered into the catalogs of critical network equipment and specialized cybersecurity products, and must pass testing and certification by qualified bodies before being sold or provided. Testing and certification of commercial cryptography products is to apply the relevant provisions of the 'People's Republic of China Cybersecurity Law', to avoid repetitive testing." 2019 Cryptography Law, Article 26.

addition, Article 24 states, "[c]ommercial cryptography work units launching commercial cryptography activities shall comply with the technical requirements of relevant laws, administrative regulations, compulsory state standards on commercial cryptography, as well as the unit's public standards."[389] The Companies argue that "[t]he 2019 Cryptography Law referenced in the [*Institution Order*] states that cooperation between foreign and Chinese entities regarding commercial encryption will be voluntary and Article 31 of the law bars the State Cryptography Administration and related agencies from demanding source codes and other proprietary information related to cryptography."[390] The Companies' statements do not accurately reflect the text of the cited provisions,[391] and the provisions cited by the Companies do not limit the authority of the Chinese Communist Party under this law. On the contrary, the 2019 Cryptography Law underscores the role of the Chinese Communist Party, as reflected in Article 4 which states, "[t]he cryptography leadership body of the Party Central Committee carries out uniform leadership the entire nation's cryptography work . . . ."[392] In fact, Article 3 states, among other things, that "[c]ryptography work adheres to an overall national security perspective."[393] Further, a Deputy Assistant Attorney General for the U.S. Department of Justice, National Security Division, stated that "[n]one of these laws provide much, if any, detail about legal procedures or judicial oversight available to challenge Chinese government demands," and "[t]hese laws are not merely defensive in nature: they enable the Chinese government to make affirmative demands on its people and entities to advance the Communist Party's interest."[394] The Companies offer no persuasive argument to refute the concerns raised by the

[389] 2019 Cryptography Law, Article 24. Furthermore, Article 27 states, in part, "[w]here operators of critical information infrastructure purchase network products or services that involve commercial cryptography, and might impact national security, they shall follow the provisions of the 'People's Republic of China Cybersecurity Law' to pass national security review organized by the State Internet Information Department, together with the State Cryptography Administration, and other relevant departments." *Id*., Article 27. Such provisions further underscore the serious consequences of requirements that are imposed by the Chinese government through the 2019 Cryptography Law. *See, e.g.*, U.S. Department of Homeland Security, Office of Strategy, Policy, and Plans, Office of Trade and Economic Security, Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China at 8 (Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf (DHS Data Security Business Advisory) (warning in a public advisory that, pursuant to the 2019 Cryptography Law, which went into effect in January 2020, "[a]ny encryption system that is 'approved' for use in China, or by companies that handle Chinese data, is required to provide its encryption keys to the [Chinese] government"); *see infra* note 394.

[390] PN/CN April 28, 2021 Reply at 11-12 (citing 2019 Cryptography Law, Articles 21 and 31).

[391] The provision of Article 21 to which the Companies refer states, in part, "[a]ll levels of people's government and their relevant departments shall follow the principle of nondiscrimination to lawfully give equal treatment to units, including foreign investment enterprises, such as those researching, producing, selling, servicing, or importing or exporting, commercial cryptography (hereinafter jointly referred to as 'commercial cryptography work units'). The state encourages technological cooperation on commercial cryptography to be conducted in the course of foreign investment and on the basis of the voluntariness principle and business rules." 2019 Cryptography Law, Article 21. The text of this provision does not display the language suggested by the Companies, "cooperation between foreign and Chinese entities." The provision of Article 31 to which the Companies refer states, in part, "[c]ryptography management departments and relevant departments, as well as their staffs, must not require commercial cryptography work units and commercial cryptography testing and certification bodies to disclose source code and other proprietary information related to cryptography . . . ." *Id*., Article 31. The text of the provision does not display the language suggested by the Companies, that "the State Cryptography Administration and related agencies" are barred from "demanding" source code and other propriety information related to cryptography. *See also infra* note 395.

[392] 2019 Cryptography Law, Article 4.

[393] *Id*., Article 3.

[394] Statement of Deputy Assistant Attorney General Adam S. Hickey at 7 (discussing the 2017 Cybersecurity Law, 2017 National Intelligence Law, and 2019 Cryptography Law); *see supra* paras. 58-62 (discussing the ties of the (continued….)

record that the Chinese government could require the Companies to take certain actions pursuant to the 2019 Cryptography Law, or other laws, through the Chinese government's ownership and control of the Companies' parent entities, and consequently, the Companies.

72. Lastly, we reject the Companies' argument that "the [*Institution Order*] tries to ignore the actual application of the 2018 Company Law by pointing to the allegedly coercive effect of the laws discussed above."[395] We find that the 2018 Company Law further affirms the significant national security and law enforcement concerns that are presented by the influence and control of the Chinese Communist Party and the compliance required of companies pursuant to this law with respect to the Chinese Communist Party's priorities and goals.[396] The Companies argue that the 2018 Company Law is inapplicable in this case because "Article 64 [of the 2018 Company Law] makes clear that if a company is 'invested *wholly* by the state,' it is subject to special provisions—provisions not applicable to the Companies that are only partially owned by the Chinese government."[397] The Companies contend that they "are not subject to certain provisions of China's 2018 Company Law that would increase the control of the Chinese government over mergers, dissolutions, and other important decisions by wholly state-owned enterprises."[398] The Companies have not disputed, however, that their ultimate parent entity, CITIC Group Corporation is a wholly state-owned entity and subject to the 2018 Company Law.[399] The 2018 Company Law regulates "the organization and operation of companies," which specifically includes "a limited liability company," and would apply to CITIC Group Corporation.[400] As stated in the *Order to*

(Continued from previous page)
Companies' indirect parent entities to the Chinese Communist Party and the Chinese Government). Moreover, the Companies do not address the full provision of Article 31 of the 2019 Cryptography Law, which further states, "[c]ryptography management departments and relevant departments are to establish systems for regulation of commercial cryptography, during and after the fact, that combine routine oversight and random sampling inspections, establish a unified platform for commercial cryptography oversight and management information, advance the establishment of connections between regulation during and after the fact and the social credit system . . . ." 2019 Cryptography Law, Article 31; *see* DHS Data Security Business Advisory 8 ("Specifically, Article 31 of the Cryptography Law allows the [State Cryptography Administration] to request complete access to commercial cryptography systems, including to the data protected by such systems. The result is that the [State Cryptography Administration] has full access to decryption keys, passwords, and any other information needed to access data on a commercially encrypted server."); Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020 at 22 (Nov. 3, 2021), https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF (stating that the 2019 Cryptography Law "provides for the State Cryptography Administration and its local agencies to have complete access to cryptography systems and the data protected by those systems"); *see also* PN/CN April 28, 2021 Reply at 11-12.

[395] PN/CN April 28, 2021 Reply at 12.

[396] *See* Company Law of the People's Republic of China (2018 Amendment), Article 19. The Revised Constitution of the Communist Party of China sets forth, among other things, that "[l]eadership of the Communist Party of China is the most essential attribute of socialism with Chinese characteristics, and the greatest strength of this system" and "[t]he Party exercises overall leadership over all areas of endeavor in every part of the country." Revised Constitution of the Chinese Communist Party at 10; *see supra* note 328.

[397] PN/CN June 1, 2020 Response at 22-23.

[398] PN/CN April 28, 2021 Reply at 12. The Companies assert that "[a]s the [*Order to Show Cause*] Response pointed out, though, and which the [*Institution Order*] sidesteps, both CITIC Limited and [CITIC Tel] have substantial percentages of public ownership, and thus neither of the Companies are wholly state-owned." *Id.*

[399] *Id*. at 43 (disclosing to the Commission for the first time that "[t]he Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation"). *See also Order to Show Cause*, 35 FCC Rcd at 3735, 3736, paras. 4, 6 & nn.15, 23; *Institution Order*, 36 FCC Rcd at 6394, para. 38.

[400] *See* Company Law of the People's Republic of China (2018 Amendment), Article 1 ("This Law is enacted for the purposes of regulating the organization and operation of companies . . . ."); *id.*, Article 2 ("The term 'company' as (continued….)

Show Cause and the *Institution Order,* based on the Companies' *pro forma* notifications filed in 2012, CITIC Group Corporation is "a state-owned limited liability company."[401] Moreover, CITIC Group Corporation has publicly affirmed its commitment to the 2018 Company Law in its corporate governance.[402] We find, based on the record, that the Companies' ultimate parent entity must comply with the 2018 Company Law, and consequently, the risks to U.S. national security and law enforcement interests associated with such compliance are substantial.[403] Significantly, Article 19 of the 2018

(Continued from previous page)
mentioned in this Law refers to a limited liability company or a joint stock company limited set up within the territory of the People's Republic of China according to the provisions of this Law").

[401] 2012 Pacific Networks Pro Forma TC Notification, Attach. 1 at 1-2, Exhs. A, B (stating that "CITIC Group Corporation (formerly known as CITIC Group) has taken the several restructuring actions detailed below," involving, among other things, "[t]he transformation of CITIC Group from a state-owned enterprise into CITIC Group Corporation, a state-owned limited liability company, which involved a change of the company's industrial and commercial registration . . . ."); 2012 ComNet Pro Forma TC Notification, Attach. 1 at 1-2, Exhs. A, B (stating that "CITIC Group Corporation (formerly known as CITIC Group) has taken the several restructuring actions detailed below," involving, among other things, "[t]he transformation of CITIC Group from a state-owned enterprise into CITIC Group Corporation, a state-owned limited liability company, which involved a change of the company's industrial and commercial registration . . . ."); *Order to Show Cause*, 35 FCC Rcd at 3735, para. 4 & n.14; *Institution Order*, 36 FCC Rcd at 6372, para. 5; *see CITIC Group Corporation Corporate Governance and Risk Management*.

[402] *CITIC Group Corporation Corporate Governance and Risk Management* ("In accordance with the Company Law and the Articles of Association, the Group further improved its governance structure in line with modern business operations, and the checks and balances among the Board of Directors, the Board of Supervisors and the Management, to provide the mechanisms necessary for operation efficiency"); *Institution Order*, 36 FCC Rcd at 6389-90, para. 33 & n.142 (quoting *CITIC Group Corporation Corporate Governance and Risk Management*).

[403] While it does not alter our conclusion that the Companies' ultimate parent entity is subject to the 2018 Company Law, we note that an English language translation of Article 64 defines a "'wholly state-owned company' as mentioned in this Law" as "a limited liability company invested wholly by the state, for which the State Council or the local people's government authorizes *the state-owned assets supervision and administration institution of the people's government at the same level to perform the functions of the capital contributor*." 2018 Company Law (Amendment 2018), Article 64 (emphasis added) (codified in "Chapter II Establishment and Organizational structure of A Limited Liability Company") (stating, "[t]he provisions of this Chapter shall apply to the establishment and organizational structure of the wholly state-owned companies. Any matter not covered by this Chapter shall be governed by the provisions of Sections 1 and 2 of this Chapter."). The Bureaus stated in the *Order to Show Cause*, "[SASAC], a Chinese government organization, directly owns 100% of CITIC Group Corporation." *Order to Show Cause*, 35 FCC Rcd at 3735, para. 4. In support of this statement, the Bureaus cited to *pro forma* transfer of control notifications that were filed on behalf of Pacific Networks and ComNet in 2012. *Id.* Additionally, the *Order to Show Cause* stated, "Pacific Networks and ComNet, like China Mobile USA, are subject to the supervision of [SASAC]" and cited, among other matters, to Article 64 of the 2018 Company Law. *Id.* at 3736, para. 6, n.23. In the *Institution Order*, the Commission stated, "[a]s we noted in the *Order to Show Cause*, the Commission's records reflect that [SASAC], a Chinese government organization, directly owns 100% of CITIC Group Corporation and Pacific Networks and ComNet do not dispute that their ultimate parent entity is subject to the 2018 Company Law or that it is a wholly state-owned entity," and noted, "Pacific Networks and ComNet failed to provide 'a detailed description of the current ownership and control (direct and indirect)' held by the Chinese government in the ultimate parent entity, and consequently Pacific Networks and ComNet." *Institution Order*, 36 FCC Rcd at 6394, para. 38 & n.180. In their response to the *Institution Order*, the Companies now state that the Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation without any explanation as to why they previously represented to the Commission that SASAC directly owns 100% of CITIC Group Corporation or when the change occurred. *See* PN/CN April 28, 2021 Reply at 43. While Article 64 applies to entities in which "the state-owned assets supervision and administration institution of the people's government at the same level . . . perform[s] the functions of the capital contributor"—and to the extent that this language pertains to SASAC—we find that the 2018 Company Law nonetheless applies to the Companies' ultimate parent entity for the reasons stated herein. We further note that, in line with their failure to fully respond to the *Order to Show Cause* and the *Institution Order*, as discussed in Section III.B.3., the Companies did not address the full provision of Article 64 in their arguments and even stated in their response to the *Order to Show Cause*,
(continued….)

Company Law states, "[t]he Chinese Communist Party may, according to the Constitution of the Chinese Communist Party, establish its branches in companies to carry out activities of the Chinese Communist Party."[404] Article 19 adds that "[t]he company shall provide necessary conditions to facilitate the activities of the Party."[405] As discussed above, CITIC Group Corporation has a Chinese Communist Party organization within its corporate leadership, the leaders and members of which hold positions on the Board of Directors, Board of Supervisors, and Senior Management.[406] Overall, the Companies failed to provide any evidence to dispel the significant concerns associated with the ties of their indirect parent entities with the Chinese Communist Party and the Chinese government, and, consequently, the influence and control of such Chinese governing authorities on the Companies.

73. As we stated in other proceedings, we find that the combination of Chinese cybersecurity and national intelligence laws presents serious and substantial national security and law enforcement concerns regarding the Companies' vulnerability to exploitation, influence, and control by the Chinese government.[407] Based on the overall record evidence, we find that the Companies' retention of their section 214 authority raises substantial national security and law enforcement risks because of these identified laws and the Chinese government's relationship with the Companies' parent entities.[408] For the reasons described in this Order, revocation is both appropriate and necessary in this case.[409]

(Continued from previous page)
without clarifying their actual ownership and control, that "[t]he [*Order to Show Cause*] states that the Companies 'are subject to the supervision of the State-owned Assets Supervision and Administration Commission of the State Council, a Chinese government organization,' then notes that Article 64 of the 2018 Company Law applies to a 'wholly state-owned company' . . . Specifically, the Company Law states that the bylaws of wholly state-owned companies must be formulated or approved by the state-owned assets supervision and administration institution . . . ." PN/CN June 1, 2020 Response at 22-23 (citing 2018 Company Law (Amendment 2018), Articles 65, 66).

[404] Company Law of the People's Republic of China (2018 Amendment), Article 19.

[405] *Id*.; *Institution Order*, 36 FCC Rcd at 6389-90, para. 33 & nn.142-143; *see supra* note 330.

[406] *See supra* paras. 60-61. Additionally, we discuss above the overlap in the corporate leadership of CITIC Group Corporation and its subsidiaries, CITIC Limited and CITIC Tel. *See supra* para. 50.

[407] *See China Telecom Americas Order on Revocation and Termination* at *22, para. 60 ("The combination of these laws—the 2017 Cybersecurity Law, the 2018 Cybersecurity Regulation, and the 2017 National Intelligence Law—raises substantial and serious national security risks."); *id.* at *23, para. 63; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 67 (finding that "the combination of these laws—the 2017 Cybersecurity Law, the 2018 Cybersecurity Regulation, the 2017 National Intelligence Law, and the 2019 Cryptography Law—raises serious and significant national security risks"); *id.* at paras. 64-65, 69-71.

[408] We note that the Companies argue that "[j]ust as Team Telecom signed off on the 2009 Letter of Assurance to address national security concerns that existed at that time, so too could Team Telecom have at least attempted to the same to address the change [sic] national security environment stemming form [sic] adoption of Chinese law in the intervening years." PN/CN April 28, 2021 Reply at 20. As discussed below, we find that these risks cannot be mitigated, contrary to the Companies' assertions. *See infra* Section III.D; Executive Branch June 4, 2021 Reply at 3 ("Any mitigation agreement, no matter how complex or simple, requires a baseline level of trust between the relevant parties to the agreement, because the requisite oversight necessary to assess compliance would not necessarily be adequate to detect intentional, and possibly state-sponsored, efforts to surreptitiously violate mitigation measures. That level of trust is absent here. The Monitoring Agencies simply lack confidence that the Companies' corporate chain will choose to meet their mitigation obligations when faced with an order from the Chinese government.").

[409] The Companies argue, "the Cybersecurity and National Intelligence Laws have already been in force for four years, and the 2019 Cryptography Law has been in force for a year and a half. And yet there has not been a single reported instance of either of the Companies or any of their employees ignoring their obligations under U.S. law in response to a demand from the Chinese government." PN/CN June 28, 2021 Reply at 3. Our actions herein are based on our public interest analysis, which considers, among other things, the changed national security

(continued….)

2. The Companies' Retention of Section 214 Authority Presents National Security and Law Enforcement Risks

74. Given the changed national security environment since the Commission authorized the Companies to provide telecommunications services in the United States and based on our review of the full record in this proceeding, we conclude that the significant national security and law enforcement risks associated with the Companies' retention of their section 214 authority pose a clear and imminent threat to the security of the United States. As explained below, the Companies' operations in the United States pursuant to their domestic and international section 214 authority, which may be enhanced by those operations that do not require section 214 authority, provide the Companies with access to U.S. telecommunications infrastructure and sensitive U.S. customer information. As the Executive Branch agencies observe, "[t]he Companies, as international [s]ection 214 authorization holders, are connected to the domestic telecommunications networks of the United States and have direct access to the telephone lines, fiber-optic cables, cellular networks, and communications satellites that constitute those networks."[410] These connections and access present the Companies, their parent entities, and therefore the Chinese government, with numerous opportunities to access, monitor, store, and in some cases disrupt and/or misroute U.S. communications, which in turn allow them to engage in espionage and other activities harmful to U.S. national security and law enforcement interests.[411] Because the Chinese government has influence and control over the Companies, as discussed above, the record raises serious and unacceptable concerns that the Chinese government can, for example, direct or otherwise influence the Companies to act on opportunities presented by their access to U.S. telecommunications infrastructure and U.S. customer information.[412] Despite being afforded several opportunities to address these national security and law enforcement risks, the Companies failed to persuasively dispute or explain how they can be ameliorated.[413] Indeed, the Companies did not adequately refute the national security and law enforcement concerns that we raised in the *Institution Order*.[414] Accordingly, we conclude that the Companies' retention of section 214 authority presents national security and law enforcement risks that warrant revocation of their section 214 authority.

75. As described above, the Companies have blanket domestic section 214 authority and both Pacific Networks and ComNet hold an international section 214 authorization.[415] Pacific Networks is authorized to provide resale service on all U.S. international routes, except for the U.S.-China and U.S.-Hong Kong routes, on which it is authorized to provide switched services solely through the resale of unaffiliated U.S. facilities-based carriers' international switched services (either directly or indirectly through the resale of another U.S. resale carrier's international switched services).[416] ComNet is authorized to provide both facilities-based and resale service between the United States and all

(Continued from previous page)
environment since the Companies' section 214 authorizations were granted and the national security and law enforcement risks identified in the record. Further, as we discuss below, the record demonstrates that the national security and law enforcement concerns identified are not a "theoretical potential." PN/CN June 1, 2020 Response at 21; *see infra* Section III.B.2.

[410] Executive Branch Nov. 16, 2020 Letter at 10.

[411] As discussed below, while the Companies currently have the ability to access, monitor, store, and in some cases disrupt and/or misroute communications, Pacific Networks and ComNet appear not to have the ability to misroute communications using Border Gateway Protocol (BGP), a well-known security threat. *See infra* para. 80.

[412] *See supra* Section III.B.1.

[413] *See supra* para. 28.

[414] *See Institution Order*, 36 FCC Rcd at 6396-6404, paras. 41-51.

[415] *See supra* para. 6.

[416] *Order to Show Cause*, 35 FCC Rcd at 3742-43, Appx. A, paras. 5-6; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384.

permissible foreign points, except for the U.S.-China and U.S.-Hong Kong routes, where it is authorized to provide switched services solely through the resale of unaffiliated U.S. facilities-based carriers' international switched services (either directly or indirectly through the resale of another U.S. resale carrier's international switched services).[417]

76. The Companies state that pursuant to their domestic and international section 214 authority, ComNet provides Retail Calling Card service[418] and Wholesale IDD service,[419] and Pacific Networks provides MPLS VPN service.[420] The Companies are authorized to, at any time, provide any other domestic service under blanket domestic section 214 authority,[421] and to provide "international basic switched, private line, data, television and business services" pursuant to section 214 authority and in compliance with their specific international section 214 authorizations.[422] Significantly, this authority allows a carrier to extend its network in the United States, install new equipment or upgrade existing equipment on its network, or request additional interconnections with the networks of other U.S. common carriers—all without seeking further Commission approvals.

77. As the Executive Branch agencies have observed and the Commission has recognized, circumstances have changed dramatically since 2009 when the Commission last granted the Companies section 214 authorizations to provide international common carrier services.[423] According to the Executive Branch agencies, in 2009, "the U.S. Intelligence Community's top concerns were the global economic crisis and violent extremism," and while the annual threat assessment of the Office of the Director of National Intelligence (ODNI) briefly noted the threat to U.S. information infrastructure from adversaries, "China's role in this growing threat was only mentioned in passing."[424] The current threats

[417] *Order to Show Cause*, 35 FCC Rcd at 3734, para. 2; *id.* at 3740-42, Appx. A, paras. 2-4; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379; May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784.

[418] *See* PN/CN April 28, 2021 Reply at 56 ("As ComNet's Retail Calling Card service facilitates international calls, the Companies consider it to be provided pursuant to ComNet's international Section 214 authority."). The Companies clarify that there is only limited use of this service for domestic telecommunications, and in such cases, the service is provided pursuant to ComNet's blanket domestic section 214 authority. *See id*. at 55 ("Please note that for ComNet's Retail Calling Card and Wholesale IDD services . . . , these services are almost entirely used for international calls. It is possible, however, for the services to route U.S. domestic traffic, although this is a minimal amount of the traffic handled by the services. To the extent, then, that these services can facilitate domestic calls within the U.S. and a minimal amount of such calls are handled, the Companies consider these services to also be provided pursuant to ComNet's blanket domestic 214 authority.").

[419] *See id*. at 56 ("The Companies consider this service to be provided pursuant to ComNet's international Section 214 authority.").

[420] *See id*. at 55 ("Pacific Networks' MPLS VPN service provides data communications that enable its customers to operate business applications among various customer sites both within the United States and internationally. To the extent this service makes use of domestic facilities and routes traffic within the U.S., the Companies consider it to also be provided pursuant to Pacific Networks' blanket domestic 214 authority."); *id*. at 56 ("While Pacific Networks does not itself provide international circuits required for MPLS VPN, to the extent Pacific Networks' MPLS VPN service facilitates the exchange of international traffic, the Companies consider it to be provided pursuant to Pacific Networks' international Section 214 authority.").

[421] 47 CFR § 63.01.

[422] 47 CFR §§ 63.22(d), 63.23(c); 47 U.S.C. § 214; 47 CFR § 63.18(e)(1)-(2).

[423] Executive Branch Nov. 16, 2020 Letter at 2; *Institution Order*, 36 FCC Rcd at 6397, para. 42; *see China Telecom Americas Order on Revocation and Termination* at *25, para. 67; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 76.

[424] Executive Branch Nov. 16, 2020 Letter at 2-3 (citing *Annual Threat Assessment of the Intelligence Comm. For the S. Select Comm. on Intelligence*, 111th Cong. 38-39 (2009) (statement of Dennis C. Blair, Director of National Intelligence), https://www.dni.gov/files/documents/Newsroom/Testimonies/20090212_testimony.pdf).

facing the United States are significantly different and extremely serious, including increasing cyber-attacks against the United States. According to ODNI's 2019 annual threat assessment, China is "the first country identified by name for its persistent economic espionage and growing threat to core military and critical infrastructure systems."[425] ODNI's 2021 annual threat assessment observed that "China will remain the top threat to US technological competitiveness" and that the Chinese government employs "a variety of tools, from public investment to espionage and theft, to advance its technological capabilities."[426] ODNI continues to find that "China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat."[427] Additionally, in recent years, the U.S. government has issued numerous official statements, testimonies, reports, and criminal indictments that highlight the significantly enhanced national security threat associated with the Chinese government's activities. For instance, the Executive Branch agencies state that, according to DOJ charging documents, "about 80 percent of economic espionage cases (which allege trade secret theft intended to benefit a foreign state) implicate the Chinese state (as opposed to another country), and about two-thirds of DOJ's trade secrets cases overall have some nexus to China."[428] Similarly, the Director of the Federal Bureau of Investigation "warned that 'no country poses a broader, more severe intelligence collection threat than China.'"[429] The Office of the U.S. Trade Representative (USTR), in its 2018 Section 301 Report, stated that "cyber theft became one of China's preferred methods of collecting commercial information because of its . . . plausible deniability."[430] The USTR, in its 2021 Section 301 Report, indicated that China remains on its Priority Watch List and is one of only nine countries so designated.[431] Importantly, the Executive Branch agencies warn that the threat from Chinese government-sponsored cyber actors is not only limited to direct acts by the Chinese government, "but also include[s] its potential use of Chinese information technology firms as routine and systemic espionage platforms against the United States."[432]

---

[425] *Id*. at 3 (citing 2019 ODNI Threat Assessment at 5). *See also Institution Order*, 36 FCC Rcd at 6397, para. 42.

[426] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* at 7 (April 9, 2021), https://go.usa.gov/x6M7g.

[427] *Id.* at 8. Among other threats, ODNI's 2021 assessment observes that "China's cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US homeland . . . " and that "China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations." *Id.*

[428] Executive Branch Nov. 16, 2020 Letter at 4-5; *see Institution Order*, 36 FCC Rcd at 6397-98, para. 42 & n.206. The Executive Branch agencies also cite to incidents of public law enforcement actions against Chinese actors. Executive Branch Nov. 16, 2020 Letter at 5.

[429] Executive Branch Nov. 16, 2020 Letter at 4 (quoting Christopher Wray, Dir. Fed. Bureau of Investigation, Address at the Ninth Annual Financial Crimes and Cybersecurity Symposium, Keeping our Financial Systems Secure: a Whole-of-Society Approach, at 2 (Nov. 1, 2018) (transcript *available at* https://go.usa.gov/xeAqq)).

[430] USTR 2018 301 Report at 153; Executive Branch Nov. 16, 2020 Letter at 4.

[431] Office of the U.S. Trade Representative, Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974 at 5 (Apr. 2021) (2021 301 Report), https://go.usa.gov/xeFMN. The Report notes that, "[s]ince enacting its Cybersecurity Law in 2017, China has continued to build on its policies for 'secure and controllable' Information Communications Technology (ICT) products, such as the issuance of the Cybersecurity Classified Protection Scheme in May 2020. Along with the adoption of the Cryptography Law in 2019 and the Cybersecurity Review Measures in 2020, these developments represent multiple steps backward through China's efforts to invoke cybersecurity as a pretext to force U.S. IP-intensive industries to disclose sensitive IP to the government, transfer it to a Chinese entity, or restrict market access." *Id*. at 48.

[432] Executive Branch Nov. 16, 2020 Letter at 9 (citing 2019 ODNI Threat Assessment at 5); *see Institution Order*, 36 FCC Rcd at 6397, para. 42.

a. The Companies' Section 214 Operations Provide Them Enhanced Opportunity and Ability to Access, Monitor, Store, and in Some Cases Disrupt and/or Misroute U.S. Communications

78. Based on the totality of the evidence in the record, we find that the variety of services that are offered or could be offered by the Companies pursuant to their section 214 authority, which may be enhanced by those services that do not require section 214 authority, provide the Companies with access to U.S. telecommunications infrastructure and U.S. customer records. This access presents the Companies, their controlling parent entities and their affiliates, and the Chinese government with opportunities to access, monitor, store, and in some cases disrupt and/or misroute U.S. communications and the opportunity to facilitate espionage and other activities harmful to the interests of the United States.[433] According to the Companies, as noted above, ComNet provides Retail Calling Card and Wholesale IDD services pursuant to its section 214 authority as well as other non-section 214 services, while Pacific Networks provides only MPLS VPN service, which it provides pursuant to its section 214 authority.[434] ComNet's non-section 214 services include resale of prepaid mobile data SIM cards, VoIP, and Wholesale SMS.[435] ComNet also indicates that it has underlying infrastructure that supports VoIP[436] {[ ]}[437] ComNet's section 214 services could be offered with other related non-section 214 services and marketed collectively,[438] thus potentially increasing the Companies' appeal to more customers. Although the Companies' infrastructure is geographically limited, it provides significant connectivity between the United States, {[ ]}[439] The PSI Report observed that "ComNet has only one point of presence in the United States, located in Los Angeles, California," yet also recognized that "Team Telecom records describe the Los Angeles facility

[433] *See supra* at Section III.B.1. According to the March 22, 2018 presentation to DOJ, {[ ]} *See* PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-10.

[434] *See supra* para. 76.

[435] *See* PN/CN June 1, 2020 Response at 14-15. With respect to the resale of prepaid mobile data SIM cards, the Companies state that, "in reselling SIM cards, ComNet acts identically to any other retail distributor of these products." *Id*. at 15. With respect to ComNet's VoIP service, the Companies state that "[t]he Commission has not required providers to obtain Section 214 authorizations for the provision of interconnected VoIP." *Id*. at 14. With respect to ComNet's Wholesale SMS service, the Companies maintain that, "[a]s an information service, ComNet does not require a Section 214 authorization to provide this service." *Id*. *See id*., Business Confidential Exh. E ("Customers"); PN/CN April 28, 2021 Reply, Business Confidential Exh. H ("Revised Customer Lists").

[436] PN/CN April 28, 2021 Reply at 82-83.

[437] PN/CN June 1, 2020 Response, Business Confidential Exh. D at D-2-D-5; *see infra* note 536. {[ ]}

[438] *See, e.g*., LinkedIn, ComNet, https://www.linkedin.com/company/comnet-telecom/about/ (last visited Mar. 1, 2022) ("[ComNet] was established in 1999, offering telecom partners and operators international termination services, calling card and global SIM card in an era of booming communications demand. As Information and Communications Technology (ICT) revolution and marketing transformation, several years ago, we engaged into and specialized in ICT field by providing enterprise business phones system, A2P SMS, managed network and IT service, website and WeChat related development, etc. We have been proudly serving the customers in North America for more than 20 years."). *See also* Facebook, ComNet, https://www facebook.com/Comnet.us/ (last visited Mar. 14, 2022).

[439] PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-15.

as 'the premier communications hub of the Pacific Rim and arguably the single most important point of connectivity in the Western United States.'"[440]

79. We agree with the Executive Branch agencies' assessment of national security and law enforcement risks, and we find that the Companies' offerings of section 214 and non-section 214 services provide the Companies with the opportunity to engage in harmful conduct against U.S. interests.[441] The *Institution Order* summarized the Executive Branch agencies' concerns with respect to the Companies. The Executive Branch agencies state that "similar to [China Mobile USA's] anticipated customers, the Companies' customers also include fixed and mobile network operators, wholesale carriers, and calling card customers," and that "[t]he Executive Branch judged that the Chinese government could exploit [China Mobile USA's] interconnections and access to U.S. companies and data."[442] Further, the Executive Branch agencies state that "[t]he Companies' similar interconnections and customers present the same opportunity for exploitation by the Chinese government, including the ability to conduct or to increase economic espionage and collect intelligence against the United States."[443] The Executive Branch agencies assert that "[t]he [Chinese] government could use the Companies' common carrier status to exploit the public-switched telephone network in the United States and increase intelligence collection against U.S. government agencies and other sensitive targets that depend on this network."[444] Finally, the Executive Branch agencies indicate that "due to least-cost routing, the communications of U.S. government agencies to any international destinations may conceivably pass through the Companies' network during transit, even if the agencies are not actual customers of the Companies."[445] The *Institution Order* also included our independent concern, as the expert agency with respect to communications technology, that service providers such as the Companies, by virtue of controlling the systems and infrastructure used to provide the services described herein, "are in a unique position to use this access to exploit their customers' vulnerabilities on the network and, unlike other service providers with similar systems or infrastructure, may be directed to do so."[446] Ultimately, we find that the record evidence raises significant concerns that, due to their majority ownership and control by the Chinese government, the Companies and their parent entities and affiliates may be required to use the Companies' access to U.S. telecommunications infrastructure in ways that threaten the national security and law enforcement interests of the United States.[447]

80. As discussed below, the opportunities for harmful conduct exist in two categories. *First*, as a provider of Retail Calling Card service, ComNet has the opportunity to access Personally Identifiable Information (PII), Customer Proprietary Network Information (CPNI), Call Detail Records (CDRs) and/or metadata from traffic transiting ComNet's service.[448] *Second*, as a provider of Wholesale IDD service and MPLS VPN service, ComNet and Pacific Networks, respectively, have the opportunity to

[440] PSI Report at 98 (citing DHS00460PSI-65, at DSH00463PSI; DHS00466-71, at DHS00468PSI).

[441] *See generally* Executive Branch Nov. 16, 2020 Letter.

[442] Executive Branch Nov. 16, 2020 Letter at 8 (citing Executive Branch China Mobile USA Recommendation to Deny at 15); *Institution Order*, 36 FCC Rcd at 6398, para. 43 (citing Executive Branch Nov. 16, 2020 Letter at 8).

[443] Executive Branch Nov. 16, 2020 Letter at 8; *Institution Order*, 36 FCC Rcd at 6398, para. 43 (citing Executive Branch Nov. 16, 2020 Letter at 8).

[444] Executive Branch Nov. 16, 2020 Letter at 10; *Institution Order*, 36 FCC Rcd at 6398, para. 44 (citing Executive Branch Nov. 16, 2020 Letter at 10).

[445] Executive Branch Nov. 16, 2020 Letter at 10; *Institution Order*, 36 FCC Rcd at 6399, para. 44 (citing Executive Branch Nov. 16, 2020 Letter at 10).

[446] *Institution Order*, 36 FCC Rcd at 6400, para. 46.

[447] *See supra* Section III.B.1.

[448] *See infra* para. 82 (discussing PII, CPNI, CDRs, and metadata).

access, monitor, store, and in some cases disrupt and/or misroute U.S. communications. We note that our discussion concerning the ability to disrupt communications pertains to situations in which the Companies have access to the underlying data, which could include any information transmitted, such as email exchanges, voice communications, or any other application used by the Companies' customers. At present, Pacific Networks and ComNet appear not to have the ability to misroute communications using Border Gateway Protocol (BGP),[449] a well-known security threat.[450] Rather, the Companies appear to have the somewhat more limited, but nonetheless significant and dangerous, ability to access, monitor, store, and in some cases disrupt and/or misroute U.S. communications.[451] Similarly concerning is the fact that, as international section 214 authorization holders, the Companies at any time could decide to offer International Private Line Circuit (IPLC) service or International Ethernet Private Line (IEPL) service, thus raising the national security and law enforcement risks associated with these services as discussed in the *China Telecom Americas Order on Revocation and Termination*.[452] We find that the services the Companies currently provide, or could provide without further approval from or notification to the Commission, create opportunities for serious harm that present unacceptable risks to U.S. national security and law enforcement interests.

81. While we recognize that other similarly situated providers have access to customer data and have similar opportunities to engage in harmful conduct, other such providers are not identified as posing a national security and law enforcement risk like the Companies.[453] Importantly, the Companies are ultimately majority-owned and controlled by the Chinese government.[454] In light of this and the opportunities for the Companies and their parent entities and affiliates to access, monitor, store, and in some cases disrupt and/or misroute U.S communications in ways that are not authorized and that can facilitate espionage and other harmful activities, the Companies' retention of their section 214 authority presents serious and significant threats to the national security and law enforcement interests of the United States.[455]

(i) Retail Calling Card and Related Services

82. We find that ComNet's provision of Retail Calling Card service, which is offered under its section 214 authority, and ComNet's related non-section 214 service—the resale of prepaid mobile data SIM cards—provide ComNet with opportunities to access customer-related information, including PII, CPNI, CDRs,[456] and/or metadata.[457] Fundamental to protecting the security of the United States is the

[449] *See* PN/CN April 28, 2021 Reply at 60-61.

[450] *See* John Burke, *Definition: BGP (Border Gate Protocol)* (Oct., 2021), https://www.techtarget.com/searchnetworking/definition/BGP-Border-Gateway-Protocol (last visited Mar. 7, 2022) (stating that "BGP (Border Gateway Protocol) is the protocol underlying the global routing system of the internet."); *see also* Y. Rekhter et al., *A Border Gateway Protocol 4 (BGP-4)*, IETF RFC 4271 (Jan. 2006), https://datatracker.ietf.org/doc/html/rfc4271 (providing a more detailed technical description in the form of the standard).

[451] *See infra* Section III.B.2.ii.

[452] *See China Telecom Americas Order on Revocation and Termination* at *29-34, paras. 79-90.

[453] *Institution Order*, 36 FCC Rcd at 6376, para. 12 (citing Executive Branch Nov. 16, 2020 Letter at 2).

[454] *See supra* note 26 ("Based on the Companies' filings and our assessment, the Companies are indirectly 58.13% owned and controlled by CITIC Group Corporation and thus the Chinese government.").

[455] *See supra* Section III.B.1.

[456] CDRs are one example of CPNI, which includes numbers called and the frequency, duration, and timing of calls. *See* 47 U.S.C. § 222(h)(1); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6931, para. 5. "CDR" is a term of art that was initially attributed to circuit switched voice traffic; the current 2021 3GPP specifications use the term "Charging Data

(continued….)

ability to trust that a service provider will uphold the confidentiality and integrity of information.[458] Unauthorized access to such sensitive information can result in serious harms and represents a threat to U.S. national security and law enforcement interests. ComNet, like all communication services providers with access to sensitive information, has a statutory responsibility to ensure the protection of customer information, including PII[459] and CPNI.[460] In the context of CPNI, both the Communications Act and the

(Continued from previous page)
Record." A CDR represents a "formatted collection of information about a chargeable event (e.g., time of call set-up, duration of the call, amount of data transferred, etc.) for use in billing and accounting." 3rd Generation Partnership Project (3GPP), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description* (Release 16) (3GPP TS 32.298 V16.8.0) at 23 (Mar. 2021), https://www.3gpp.org/ftp/Specs/archive/32_series/32.298/32298-g80.zip (*3GPP – Charging Data Record*); 3rd Generation Partnership Project (3GPP), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Service aspects; Charging and Billing* (3G TS 22.105 version 3.2.0) at 5-6 (Oct. 1999), https://www.3gpp.org/ftp/Specs/archive/22_series/22.115/22115-320.pdf (*3GPP – Charging and Billing*) (defining "Call Detail Record (CDR)," "Charging," and "Billing"); *see ACLU v. Clapper,* 785 F.3d 787, 793 (2nd Cir. 2015) (defining "telephone metadata"); *Rural Call Completion,* WC Docket 13-39, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 16154, 16174-75, para. 42 (2013) (discussing CDRs); Alliance for Telecommunications Industry Solutions (ATIS), *call detail recording*, ATIS Telecom Glossary, https://glossary.atis.org/glossary/call-detail-recording-cdr/?search=call%20detail%20recording&page_number=&sort=ASC (last visited Mar. 8, 2022). *See also China Unicom Americas Order on Revocation*, FCC 22-9 at n.379; *China Telecom Americas Order on Revocation and Termination* at *27, n.333.

[457] At a general level, "metadata" constitute information that describes or summarizes other information to make it useful. *See* Oxford Learner's Dictionary, https://www.oxfordlearnersdictionaries.com/us/definition/english/metadata (last visited Mar. 8, 2022) (defining "metadata"). In the context of communications, "metadata" may include "a range of information, such as the source, destination and timing of a particular communication, but not its content." *See* Rohan Pearce, *Data retention: Law enforcement accessed 'metadata' more than 296k times in FY18*, ComputerWorld (July 23, 2019), https://www.computerworld.com/article/3472422/data-retention-law-enforcement-accessed-metadata-more-than-296k-times-in-fy18 html; *see also* Garry Kranz, *Definition: metadata*, Tech Target (July 2021), https://whatis.techtarget.com/definition/metadata ("Often referred to as data that describes other data, metadata is structured reference data that helps to sort and identify attributes of the information it describes.").

[458] *See* The Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* 13 (Dec. 16, 2010), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf (discussing the importance of consumer trust in network services, stating, "Trust—the belief that someone or something will behave as expected, and not another way—is of central importance to the Internet."); *see also* National Academy of Sciences, Trust in Cyberspace 2 (ed. Fred B. Schneider) (1999), https://www nap.edu/catalog/6161/trust-in-cyberspace ("Trustworthiness of an (Network Information Systems) asserts that the system does what is required—despite environmental disruption, human user and operator errors, and attacks by hostile parties—and that it does not do other things").

[459] *See TerraCom, Inc. and YourTel America, Inc.*; *Apparent Liability for Forfeiture*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13331, para. 17 (2014) (stating that "[i]n general, PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context").

[460] 47 U.S.C. § 222 ("Privacy of customer information"); *id.* § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."); *see Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Report and Order and Further Notice of Proposed Rulemaking*, 22 FCC Rcd 6927, 6931, para. 5 (2007) *(CPNI Order*) (adopting rules to ensure that CPNI is adequately protected from unauthorized access, use, or disclosure). CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B)
(continued….)

Commission's rules require telecommunications carriers and interconnected VoIP service providers to protect CPNI, which includes some of the most sensitive personal information that carriers and providers have about their customers as a result of their business relationship (e.g., phone numbers called; the frequency of calls, their duration, and the timing of such calls in terms of when they originated; and any service purchased by the consumer, such as call waiting).[461] Importantly, the Commission has taken action when service providers violate the CPNI rules, and the Commission continues to alert the public of the potential risks.[462] In the context of CDRs, the need to protect such information has long been recognized.[463] Even without revealing the content of communications, CDRs can reveal significant information.[464] According to media reports, a "massive-scale" espionage operation conducted over a period of seven years targeted and obtained CDRs (including times and dates of calls and cell-based locations) by breaking into more than 10 mobile service providers' networks around the world,[465] including Africa, Asia, Europe, and the Middle East.[466] While service providers understandably focus

(Continued from previous page)
information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." 47 U.S.C. § 222(h)(1). *See also China Telecom Americas Order on Revocation and Termination* at *27, n.325; *China Unicom Americas Order on Revocation*, FCC 22-9 at n.389 (quoting *China Unicom Americas Institution Order*, 36 FCC Rcd at 6352, n.216, and stating that "'[w]hile CPNI and PII are separately defined, they are not mutually exclusive (i.e., a carrier is privy to information due to its relationship with the customer (CPNI) that could also be used to identify the individual (PII).'").

[461] FCC, Customer Privacy, https://www.fcc.gov/general/customer-privacy (last visited Mar. 9, 2022). Section 222 of the Communications Act requires telecommunications carriers (and interconnected VoIP service providers) to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure. 47 U.S.C. § 222.

[462] *See, e.g., Annual CPNI Certifications Due March 1, 2022*, Public Notice, DA 22-117 (EB Feb. 7, 2022), https://www.fcc.gov/document/annual-cpni-certifications-due-march-1-2022 ("Because the CPNI rules provide important consumer protections, the Commission has taken enforcement action against telecommunications carriers and interconnected VoIP providers that failed to comply with the requirements, and we intend to continue to enforce the rules."); *see Sprint Corporation*, File No. EB-TCD-18-00027700, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 1655 (2020); *Verizon Communications*, File No. EB-TCD-18-00027698, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 1698 (2020); *T-Mobile USA, Inc.*, File No. EB-TCD-18-00027702, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 1785 (2020); *AT&T Inc.*, File No. EB-TCD-18-00027704, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 1743 (2020).

[463] Under U.S. law, CDRs are protected by such statutory provisions as 18 U.S.C. §§ 2701-2713, 3121-3127; 50 U.S.C. §§ 1801-1813, 1841-1846; 47 U.S.C. § 222; *see also* Florin Vancea et al., *Secure Data Retention of Call Detail Records*, 5 Int. J. of Computers, Communications, & Control 961-63 (2010), https://pdfs.semanticscholar.org/734d/d4623b8d8880f9d38dbbe2b7ab32c04a8750.pdf (Secure Data Retention of Call Detail Records); D. Richard Kuhn et al., *Security Considerations for Voice Over IP Systems: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-58, Section 2.5 Privacy and Legal Issues with VoIP (Jan. 2005), https://nvlpubs nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-58.pdf.

[464] *See ACLU v. Clapper*, 785 F.3d at 794 (reviewing argument by appellants and amici about "the startling amount of detailed information metadata can reveal—'information that could traditionally only be obtained by examining the contents of communications' and that is therefore 'often a proxy for content' . . . For example, a call to a single purpose telephone number such as a 'hotline' might reveal that an individual is: a victim of domestic violence or rape; a veteran; suffering from an addiction of one type or another; contemplating suicide; or reporting a crime. Metadata can reveal civil, political, or religious affiliations; they can also reveal an individual's social status, or whether and when he or she is involved in intimate relationships.") (citations omitted). *See also* Zack Whittaker, *Hackers are stealing years of call records from hacked cell networks*, TechCrunch (June 24, 2019), https://techcrunch.com/2019/06/24/hackers-cell-networks-call-records-theft/ (Whittaker).

[465] Whittaker; *see also* Jon Porter, *Hackers steal call records from cell providers in 'massive-scale' espionage*, The Verge (June 25, 2019), https://www.theverge.com/2019/6/25/18744020/operation-softcell-hack-call-detail-records-apt10-cybersecurity-cell-network-providers (Porter).

[466] *See* Porter.

their cybersecurity efforts on the need to protect their customers' CDRs from such hacking incidents,[467] the same potential for harm exists where service providers have access to customers' CDRs and thus opportunity to misuse this information.

83. *Retail Calling Card Service.* ComNet provides Retail Calling Card service pursuant to its section 214 authority, which involves, according to the Companies, "issuing either printed or digital phone cards with a set of 10-digit PIN numbers for international and domestic voice calls accessed via local or toll free numbers."[468] In providing this service, ComNet has access to PII, CPNI, CDRs, and/or metadata, along with the opportunity to use this information contrary to U.S. interests.[469] The Companies explain that "[c]ustomer records for different types of service are handled differently"[470] and describe "how U.S. records are handled" for these services.[471] The Companies state that "ComNet provides Retail Calling Card service through its own calling card platform, which directly collects customer international direct dialed calls via direct inward dialing ('DID') numbers provided by local service providers, using VoIP SIP connections."[472] The Companies add that, "[e]nd users can thus make international calls through the provided DID numbers by entering a 10-digit PIN and destination number using their home or mobile phone."[473] The Companies explain that ComNet's Retail Calling Card service uses the same platform as ComNet's Wholesale IDD service, which is described below, and the Retail Calling Card service maintains "a total of seven active VoIP SIP connections to the {[ ]} gateway in the Los Angeles data center."[474] Additionally, pursuant to our directive in the *Institution Order*, the Companies included in their response a copy of a March 22, 2018 slide presentation to DOJ {[

]}[475]

84. We find that there are significant national security and law enforcement risks associated with ComNet's provision of Retail Calling Card service, which is offered to U.S. customers under its section 214 authority. We also find that these risks are extended to a greater number of potential customers through ComNet's resale of prepaid mobile data SIM cards, a related non-section 214 service discussed below. In particular, in its provision of Retail Calling Card service, ComNet has the opportunity to collect a substantial amount of U.S. customer information in the form of PII, CPNI, CDRs, and/or metadata. Through such access to U.S. customer information, ComNet has the ability to associate "credit or debit card number . . . and billing, shipping and contact details,"[476] with a specific customer. The PII and CPNI of ComNet's customers could be accessed and used by Chinese government officials to cross reference or associate such information with customer PII and CPNI collected from other carriers,

[467] *See, e.g.*, Secure Data Retention of Call Detail Records, *supra* note 463, at 962-66 (outlining various ways that CDR data may be attacked and how communications "operators" may combat these threats).

[468] PN/CN June 1, 2020 Response at 14.

[469] *See infra* Section III.B.2.ii.

[470] PN/CN April 28, 2021 Reply at 47.

[471] *Id*.

[472] *Id*. at 57.

[473] *Id*.

[474] *Id*. at 80.

[475] *Id*., Business Confidential Exh. D at D-20.

[476] *Id*., Business Confidential Exh. C at C-14.

including Chinese carriers, or possibly with information obtained from third party sources, including hackers.[477]

85. The risks associated with ComNet's provision of Retail Calling Card service also relate to ComNet's access to customer communications combined with access to PII and CDRs. Specifically, given that customer calls traverse ComNet's calling card platform,[478] ComNet can access the voice conversations of its customers, the metadata derived from those calls, and the PII associated with those customers. Significantly, with this service, ComNet can also {[ ]}[479] Further supporting this concern about access to customers' conversations and data that cross ComNet's calling card platform, {[ ]}[481]

[477] *See* Patricia Zengerle & Megan Cassella, *Millions More Americans Hit by Government Personnel Data Hack*, Reuters (July 9, 2015), https://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709.

[478] *See supra* para. 83.

[479] PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-48. According to the March 22, 2018 presentation to DOJ, {[ ]} *Id*. In this regard, we dismiss the Companies' argument that there is a material disputed issue as to whether they "can be trusted to 'cooperate with the U.S. government' regarding CALEA interception requests and hold in confidence the fact that such requests have been received" based on our determinations in this Order that the Companies lack the trustworthiness and reliability we expect of telecommunications carriers and notwithstanding {[ ]} PN/CN April 28, 2021 Reply at 39-40; PN/CN June 1, 2020 Response at 8; *see supra* para. 34.

[480] PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-20.

[481] *Id*. ComNet is authorized under its international section 214 authorization, ITC-214-20090424-00199, to provide "*facilities-based and resale service* in accordance with section 63.18(e)(1) and (e)(2) of the Commission's rules . . . between the United States and all permissible foreign points, except China and Hong Kong." May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784 (emphasis added); May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. On the U.S.-China and U.S.-Hong Kong routes, ComNet is authorized to provide switched services solely through the resale of unaffiliated U.S. facilities-based carriers' international switched services (either directly or indirectly through the resale of another U.S. resale carrier's international switched services) pursuant to section 63.18(e)(3). May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. {[ ]} May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379; *see* PN/CN June 1, 2020 Response at 14; PN/CN April 28. 2021 Reply at 56-62. {[ ]} PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-20. {[ ]} *Id*. at D-20; *see* PN/CN April 28. 2021 Reply at 56-62. {[

(continued….)

86. Additionally, the CDRs available to ComNet on a per call basis will include at a minimum, the destination number, the duration of the call, and calling number used to originate the call.[482] Further, PII available to ComNet will include the customer's name (as shown on ID card or passport), address, email address, telephone number, and credit card number.[483] Importantly, unauthorized access to such sensitive customer information may cause significant harms to U.S. customers. For individuals, these harms could include financial losses due to theft of credit card information, identity theft, and blackmail. For organizations, these harms could include legal liability and costs related to reimbursing customers and repairing compromised records and systems.[484] We are also concerned with the Companies' statements in their June 1, 2020 filing that "ComNet does not maintain subscriber lists but instead sells calling cards via consignment at outlets such as bookstores, newsstands and supermarkets"[485] and "ComNet is thus not aware of the identity of customers who buy calling cards."[486] We are not persuaded by the Companies' statements, as ComNet's website shows that customers have the ability to purchase "Prepaid Calling Card[s]" from ComNet's online store[487] and ComNet would know the identities of customers who purchase calling cards online.[488]

87. ComNet's provision of Retail Calling Card service raises additional significant national security and law enforcement concerns, especially given the record evidence that {[

]}[489] Specifically, with regard to these customer records, the Companies state that {[

(Continued from previous page)

]}.

See infra para. 98. {[

]} We also note that the Companies state, "CITIC Tel's SOC in Hong Kong provides first tier support for ComNet's Wholesale IDD service, Retail Calling Card service, International SMS Service and VoIP services." PN/CN April 28, 2021 Reply at 59.

[482] *See* ComNet, *Dialing Instructions Prepaid* ("Do Not Block Your Caller ID," and "Disclaimer"), https://www.comnet-telecom.us/dialing-instructions-prepaid#pinless (last visited Mar. 10, 2022).

[483] *See* ComNet, *Create an Account*, https://www.comnet-telecom.us/customer/account/create/ (last visited Mar. 10, 2022); ComNet, *General FAQs* (How do I make a purchase?), https://www.comnet-telecom.us/general-faq (last visited Mar. 10, 2022).

[484] *See* Erika McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology,* NIST Spec. Pub. 800-122 ES-1 (2010), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf (discussing risks associated with PII, stating, "[t]he escalation of security breaches involving personally identifiable information (PII) has contributed to the loss of millions of records over the past few years. Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail. Organizational harms may include a loss of public trust, legal liability, or remediation costs.").

[485] PN/CN June 1, 2020 Response at 16.

[486] *Id*.

[487] *See* ComNet, *Prepaid Calling Cards,* https://www.comnet-telecom.us/store/prepaid-calling-card html (last visited Mar. 10, 2022) (displaying ComNet's online store for prepaid calling cards).

[488] We note that even if ComNet were to sell its Retail Calling Card service solely through third parties, ComNet would still have access to the calls that traverse its network, and thus could likely access both PII and CDRs. In addition, other service options made available by ComNet, such as the rechargeable card, require customers to provide online payment, which in turn presents risks of access to PII. *See, e.g.*, ComNet, *Rechargeable Calling Card*, https://www.comnet-telecom.us/dialing-instructions-rechargeable#tips (last visited Mar. 10, 2022).

[489] PN/CN April 28, 2021 Reply at 49.

]}[490] The Companies explain that {[

]}[492] Further, as discussed below, the Companies have also failed to comply with their obligations under the 2009 LOA to "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records . . . ."[493] Based on the record, we believe that ComNet would not be able to protect this sensitive customer information from unauthorized access, including disclosure to the Chinese government or Chinese government-sponsored actors.

88. *Resale of Prepaid Mobile Data SIM Cards/Non-Section 214 Service.* The Companies state that ComNet resells prepaid mobile data SIM cards "to customers travelling outside the United States to Canada and Asian countries, as well as . . . customers in U.S."[494] The Companies state that these SIM cards "are sold through ComNet's website and distributors" and "operate entirely on other carriers' networks and do not route traffic to Pacific Networks or ComNet."[495] While the Companies state that ComNet's Retail Calling Card service is provided pursuant to ComNet's section 214 authority,[496] the Companies assert that "in reselling SIM cards, ComNet acts identically to any other retail distributor of these products."[497] We recognize that the resale of another carrier's SIM cards complements ComNet's Retail Calling Card service and also forms part of the collection of services that ComNet can offer as a communications solutions provider. This collection of services enhances ComNet's ability to attract customers who will be susceptible to national security and law enforcement risks associated with these SIM cards and other services offered by ComNet.

89. Specifically, the risks associated with ComNet's resale of the related non-section 214 prepaid mobile data SIM card service involve ComNet's access to PII and potential to use the PII that it gathers in ways that are contrary to U.S. national security and law enforcement interests. In contrast to ComNet's Retail Calling Card service, which ComNet provides under its section 214 authority, the resale of prepaid mobile data SIM cards does not present ComNet with an opportunity to access CDRs or the content of communications associated with this service. However, the resale of prepaid mobile data SIM cards can provide ComNet with access to its customers' PII, such as credit card information, addresses, or other PII that may be required to purchase the service. Under this more limited scenario, ComNet would, similar to any other vendor, have access to whatever credit card information or other information it may require its customers to provide. As an example of possible national security and law enforcement risks, the Chinese government could require ComNet to provide it with access to the PII of ComNet's customers and then attempt to leverage sensitive and relevant information, such as poor credit history, to

[490] *Id*. at 48. The Companies further state that {[
]} *Id.*

[491] *Id*. at 49.

[492] *Id*.

[493] *See infra* Section III.C.

[494] PN/CN June 1, 2020 Response at 15.

[495] *Id*.

[496] *See* PN/CN April 28, 2021 Reply at 55.

[497] PN/CN June 1, 2020 Response at 15.

target individuals who may have access to valuable information that could be used against the United States in various ways.[498]

90. We find that the risks associated with ComNet's provision of Retail Calling Card service pursuant to its section 214 authority, which include access to customers' PII, CPNI, CDRs, and/or metadata, and ComNet's resale of the related non-section 214 prepaid mobile data SIM cards, present significant threats to U.S. national security and law enforcement interests due to the Companies' majority ownership and control by the Chinese government. ComNet's access to highly sensitive customer information, combined with the Companies' vulnerability to exploitation, influence, and control by the Chinese government, presents substantial and unacceptable national security and law enforcement concerns.

(ii) Wholesale IDD, MPLS VPN, and Related Services

91. We find that the Wholesale IDD service and MPLS VPN service currently offered by ComNet and Pacific Networks, respectively, pursuant to their section 214 authority, offer substantial opportunities for ComNet and Pacific Networks and their parent entities and affiliates to access, monitor, store, and in some cases disrupt and/or misroute U.S. communications, and therefore present significant national security and law enforcement risks. These opportunities are enhanced by the Companies' ability to combine these services with other services not subject to section 214 authority, including VoIP and Wholesale SMS. For example, the network layer service of an MPLS VPN service offered by Pacific Networks, pursuant to its section 214 authority, could be used to support the application layer VoIP-related service of ComNet, which does not require section 214 authority. *First*, we discuss the national security and law enforcement risks related to ComNet's provisioning of Wholesale IDD service and other related non-section 214 services, including VoIP and Wholesale SMS. *Second*, we discuss the national security and law enforcement risks concerning Pacific Networks' provisioning of MPLS VPN service, including Pacific Networks' ability to combine its MPLS VPN service with ComNet's section 214 and non-section 214 services.

92. We find that the national security and law enforcement risks are enhanced because, as stated above, the Companies may at any time elect to provide additional telecommunications services pursuant to their section 214 authority without seeking further approval from or notifying the Commission. These findings are consistent with the concerns raised by the Executive Branch agencies that the Companies' direct access to the domestic telecommunications networks of the United States provides "a strategic capability to target, collect, alter, block, and re-route network traffic."[499] ComNet's and Pacific Networks' provision of Wholesale IDD service and MPLS VPN service, respectively, involves direct or indirect access to U.S. customer records and data that are exchanged by their customers. We address below the opportunities these services provide the Companies to access, monitor, store, and in some cases disrupt and/or misroute U.S. communications.

93. As noted above, fundamental to protecting the security of the United States is the Commission's ability to trust that a service provider will uphold the confidentiality and integrity of information. In addition to the risks related to ComNet's access to information through the provision of Retail Calling Card service, we find that there are national security and law enforcement risks related to ComNet's and Pacific Networks' provision of Wholesale IDD service and MPLS VPN service,

---

[498] *See* Ken Dilanian, *How a $230,000 debt and a LinkedIn message led an ex-CIA officer to spy for China*, NBC News (Apr. 4, 2019), https://www nbcnews.com/politics/national-security/how-230-000-debt-linkedin-message-led-ex-cia-officer-n990691.

[499] Executive Branch Nov. 16, 2020 Letter at 10 ("The Companies, as international Section 214 authorization holders, are connected to the domestic telecommunications networks of the United States and have direct access to the telephone lines, fiber-optic cables, cellular networks, and communication satellites that constitute those networks. Such connections and access can provide a strategic capability to target, collect, alter, block, and re-route network traffic.").

respectively, which are provided pursuant to the Companies' section 214 authority.[500] The risks of attacks on the confidentiality and integrity of information—or cybersecurity attacks—are significant when bad actors have access to customer traffic through the routers, switches, and/or servers (i.e., the devices) that store or forward traffic through their networks.[501] Bad actors can breach information security in multiple ways.[502] Such breaches or attacks can be characterized in two categories: active attacks and passive attacks. Active attacks consist of intrusion into victims' networks or other deliberate disruption of data and control of signaling operations, such as denial of service in the target's network(s).[503] Active attacks tend to exploit weaknesses in standardized protocols and their implementation.[504] In the case of active attacks, a service provider that is a bad actor can gain unauthorized access to the data of a potential victim (e.g., individual consumer, company, or government entity) by gaining access to the network, such as through hacking. Passive attacks involve eavesdropping and monitoring of data to collect information.[505] In the case of passive attacks, a service provider that is carrying customer traffic, or has access to metadata and customer records, can take advantage of its designated role. The service provider can exploit the trust of its customers or the Internet Service Providers (ISPs) that rely on it to carry their traffic, by monitoring, observing, and collecting customers' data and/or metadata from the traffic. Passive monitoring can compromise both unencrypted and encrypted traffic.[506] In particular, passive monitoring

[500] *See supra* notes 418, 420.

[501] *See* Federal Trade Commission, *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers,* FTC Staff Report at i (Oct. 21, 2021), https://go.usa.gov/xtrhv (stating, "As the direct gateways to this essential and ubiquitous tool, internet service providers ('ISPs') can monitor and record their customers' every online move, giving them the ability to surveil consumers and amass large amounts of information on them as they go about their daily lives."). *See also* Karen Scarfone & Peter Mell, National Institute of Standards and Technology (NIST), *Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-94 (2007), https://go.usa.gov/xeFMV (*NIST Guide to Intrusion Detection and Prevention Systems*) (discussing types of intrusions and best practices for intrusion detection and prevention). NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems pursuant to the Federal Information Security Modernization Act of 2014. *See* National Institute of Standards and Technology, *Annual Report 2019: NIST/ITL Cybersecurity Program*, NIST Special Publication 800-211 (2020), https://go.usa.gov/xeFM6.

[502] FTC, *A Look at What ISPs Know About You* (describing information collected by a network service provider).

[503] *See, e.g.*, Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, Wired (Oct. 21, 2016), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/ (discussing distributed denial of service attack (DDoS) against Dyn, an Internet infrastructure company, that subsequently caused outages for several parts of the Internet).

[504] *See, e.g.*, Gyuhong Lee, et. al., *This is Your President Speaking: Spoofing Alerts in 4G LTE Networks*, MobiSys '19: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services 404 (2019), https://dl.acm.org/doi/pdf/10.1145/3307334.3326082 (addressing one example of an exploitation of a network standard and its implementation).

[505] *See* Richard Derbyshire et al., *An Analysis of Cyber Security Attack Taxonomies*, *2018 IEEE European Symposium on Security and Privacy Workshops* 153 (2018), https://ieeexplore.ieee.org/document/8406575 (discussing the classification of cyberattacks by defining the components of cyberattacks and assessing the effectiveness of cyberattack classifications); Chris Simmons et al., *AVOIDIT: A Cyber Attack Taxonomy* (2009), https://nsarchive.gwu.edu/sites/default/files/documents/4530310/Chris-Simmons-Charles-Ellis-Sajjan-Shiva.pdf (proposing a new taxonomy to aid in identifying and defending against cyberattacks); *see also* Ismail Butun et al., *Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,* 22 IEEE Communications Surveys & Tutorials 616 (2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8897627 (categorizing attacks towards Wireless Sensor Networks and Internet of Things as "Passive Attacks" and "Active Attacks" and identifying security solutions).

[506] In the case of unencrypted end-to-end traffic, monitoring can lead to simply viewing, copying, or even altering information (data and/or voice) if no integrity protection is present. *See* Internet Engineering Task Force (IETF), *Request for Comments: 6071, Category: Informational, IP Security (IPsec) and Internet Key Exchange (IKE)*

(continued….)

can turn into a more serious form of covert surveillance called "pervasive monitoring," which network service providers are well-situated to perform.[507] For example, as part of network management—particularly security management—a service provider may use tools to conduct network intrusion[508] or perform deep packet inspection in the absence of encryption.[509] These tools can be leveraged to further enable the service provider to access content, such as listening to conversations and using the information for unauthorized activities, and even engage in espionage contrary to U.S. interests. If traffic is encrypted, these tools can be used to acquire metadata that may allow the bad actor to decrypt the traffic, which in turn would allow the bad actor to conduct an active attack.

94. *Wholesale IDD Service.* The Companies state that ComNet's Wholesale IDD service "handles international voice traffic and facilitates least cost routing for carriers located in the U.S. and in foreign locations."[510] The Companies explain that "ComNet provides Wholesale IDD transit service facilitating both inbound and outbound voice traffic by interconnecting with U.S. carrier customers at ComNet's One Wilshire Building Data Center [in Los Angeles, California] and then using VoIP SIP or T1/E1 TDM connections to route the traffic internationally."[511] In their response to the Commission's request that the Companies identify the percentage of calls using Wholesale IDD service that are sent through SIP-based VoIP as compared to using Signaling System No. 7 (SS7),[512] the Companies state that

(Continued from previous page)
Document Roadmap (February 2011), https://www.rfc-editor.org/info/rfc6071. In the case where end-to-end encryption of data is present, monitoring can extract information from metadata that are derived from encrypted traffic or through brute force decryption. *See* Alireza Bahramali et al., *Practical Traffic Analysis Attacks on Secure Messaging Applications*, Network and Distributed Systems Security (NDSS) Symposium 2020 (May 2020), https://arxiv.org/pdf/2005.00508.pdf (discussing how metadata can be useful to decrypt encrypted data); *see also* Albert Kwon et al., *XRD: Scalable Messaging System with Cryptographic Privacy*, Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation 759 (2020), https://www.usenix.org/system/files/nsdi20-paper-kwon.pdf (presenting a metadata private messaging system that provides cryptographic privacy); Katie Terrell Hanna, *Definition: brute-force attack*, TechTarget (Sep. 2021), https://searchsecurity.techtarget.com/definition/brute-force-cracking.

[507] The Internet Engineering Task Force (IETF) describes pervasive monitoring as covert "surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers," which can include "[a]ctive or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols . . . ." Internet Engineering Task Force (IETF), *Request for Comments: 7258, Category: Best Current Practice, Pervasive Monitoring Is an Attack* at 2 (May 2014), https://www.rfc-editor.org/info/rfc7258; *id.* (identifying pervasive monitoring as "an attack on the privacy of Internet users and organisations"). In addition, the Internet Architecture Board (IAB) recognizes that an entity that is well-situated, such as a network service provider, may be an "observer" in that it "is able to observe and collect information from communications, potentially posing privacy threats, depending on the context." *See* Internet Architecture Board (IAB), *Request for Comments: 6973, Category: Informational, Privacy Considerations for Internet Protocols* at 7, 11-12 (July 2013), https://www.rfc-editor.org/info/rfc6973. The IAB notes that an attacker such as an "eavesdropper" can "passively observe[] an initiator's [sender's] communications without the initiator's knowledge or authorization" in the context of compromising privacy. *Id.* at 7, 11-12.

[508] *See*, *e.g.*, *NIST Guide to Intrusion Detection and Prevention Systems*, *supra* note 501, Section 2.

[509] *See* Ericka Chickowski, *Deep packet inspection explained*, AT&T (Oct. 2, 2020), https://cybersecurity.att.com/blogs/security-essentials/what-is-deep-packet-inspection. Deep packet inspection is the ability to examine additional signaling, or the raw data, placed in various parts of the packet. *Id.*

[510] PN/CN April 28, 2021 Reply at 56.

[511] *Id.* at 57.

[512] The Commission requested that the Companies identify the percentage of calls using Wholesale IDD service that are sent through SIP-based VoIP as compared to using Signaling System No. 7 (SS7) or TDM connections. *Institution* Order, 36 FCC Rcd at 6416, Appx. A ("Pacific Networks and ComNet shall also include in their response . . . an identification of the percentage of calls using IDD service that use SS7 compared to SIP based Interconnected VoIP"). We note that the opportunities for a provider to access, monitor, store, and/or disrupt or (continued….)

"[i]n 2020, the total percentage of SS7 traffic as compared to SIP based Interconnected VoIP was less than {[ ]}% of ComNet's total Wholesale IDD service traffic."[513] The Companies further explain that ComNet {[ ]}[514] Although ComNet states that it offers Wholesale IDD service, the Internet-related resources (i.e., IP addresses and Autonomous System (AS) number) used to support ComNet's service operating over IP networks are registered by points of contact, including email and postal addresses associated with {[ ]}[515] This implies a more integrated relationship between ComNet and {[ ]} than the Companies conveyed in their responses to the *Order to Show Cause* and the *Institution Order*. Additionally, pursuant to our directive in the *Institution Order*, the Companies included in their response a copy of a March 22, 2018 slide presentation to DOJ {[ ]}[516]

95. With respect to U.S. customer records associated with ComNet's Wholesale IDD service, the Companies state that "access to records is coordinated by CITIC Tel according to the corporate policy for granting such access . . . ."[517] Significantly, the Companies did not disclose any further information on this joint coordination process, including who has the final decision-making authority in granting access to those records.[518] The Companies explain that {[ ]}[519] The Companies state that {[ ]}[520] Additionally, the "inventory of equipment" that the Companies identified for ComNet in

(Continued from previous page)
misroute communications without authorization, and thus the potential threats, vary somewhat between these technologies. In particular, SS7 uses switching systems that have long been associated with PSTN, while SIP based VoIP technologies rely on a packet-based infrastructure that can support a variety of VoIP and non-VoIP applications. The means by which a provider may engage in any of these unauthorized acts are related to how that operator's service has been engineered, i.e. using a more network-based or application-based approach.

[513] PN/CN April 28, 2021 Reply at 73.

[514] *Id*. at 62.

[515] {[ ]}

[516] PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-17; *Institution Order*, 36 FCC Rcd at 6416, Appx. A (directing the Companies to provide "a detailed description of Pacific Networks' and ComNet's domestic communications infrastructure within the United States and its connectivity to operations infrastructure within Hong Kong and China and provide a copy of what Pacific Networks and ComNet provided to DOJ as identified in a June 8, 2018 letter from DOJ to Pacific Networks and ComNet" (citing PN/CN June 1, 2020 Response, Exh. K at 156-157)).

[517] PN/CN April 28, 2021 Reply at 48.

[518] The Companies state, with respect to {[ ]} associated with ComNet's Wholesale IDD service, "[f]or this service, access to records is *coordinated* by CITIC Tel according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy." *Id*. (emphasis added).

[519] *Id*. at 47-48.

[520] *Id*. at 48.

their response to the *Order to Show Cause* {[
]}[521]

96. Based on the record evidence, we find that ComNet has the ability to access, monitor, store, and/or disrupt communications through its provisioning of Wholesale IDD service. We assess that, in the provision of this service, ComNet is likely to have access to both encrypted and unencrypted data. In cases where data are unencrypted, ComNet will have direct access and thus the opportunity to copy, monitor, store, and/or disrupt communications of its customers. In cases where data are encrypted end-to-end between clients, ComNet will have the opportunity to extract metadata from this Wholesale IDD traffic.[522] Finally, metadata in the form of CDRs are available to ComNet in its provision of Wholesale IDD service as well as the related non-section 214 services, such as VoIP and SMS.[523]

97. Above, in the discussion of CDRs associated with ComNet's Retail Calling Card service, we found that significant potential for harm exists where ComNet has access to sensitive U.S. customer records and where {[
]}[524] This same potential for harm applies to ComNet's provision of Wholesale IDD service. As discussed, the record shows how integrated ComNet's and Pacific Networks' operations—{[
]}—are with that of their indirect parent entity, CITIC Tel, and its subsidiaries, {[ ]} and how closely ComNet and Pacific Networks coordinate with these entities.[525] Additionally, the Companies state that {[
]}[526]

98. In addition, {[

[521] *See* PN/CN June 1, 2020 Response, Business Confidential Exh. D at D-2 ({[
]}); *id.* at 15 ("An inventory of the equipment used by the Companies at their locations in Los Angeles and New York is provided as Exhibit D."). *See also infra* para. 98.

[522] A network service provider monitoring encrypted traffic can gather data from who the traffic is from, where the traffic is going, how often the traffic flows, the size of the traffic, the protocols employed and other information that would not be encrypted in the header of the packet. *See* Monica Skowron et al., *Traffic Fingerprinting Attacks on Internet of Things Using Machine Learning,* 8 IEEE Access 20386 (Jan. 2020), http://doi.org/10.1109/ACCESS.2020.2969015; Noah Apthorpe et al., *Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping,* 2019 Proceedings on Privacy Enhancing Technologies 128 (2019), https://doi.org/10.2478/popets-2019-0040; Jan Kohout, Tom Pevny, *Network Traffic Fingerprinting Based on Approximated Kernel Two-Sample Test,* 13 IEEE Transactions on Information Forensics and Security 788 (2018), http://doi.org/10.1109/TIFS.2017.2768018.

[523] *See* Kevin Bartley, *What are Call Detail Records (CDRs?)*, Onsip, https://www.onsip.com/voip-resources/voip-fundamentals/what-are-call-detail-records-cdrs (last visited Mar. 10, 2022).

[524] *See supra* paras. 84-87.

[525] *See supra* paras. 53, 65.

[526] *See supra* paras. 56, 95; PN/CN April 28, 2021 Reply at 47-48.

[527] PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-17; *id.* at 49 ({[

(continued….)

]}[529] The {[
]}[530] With the inclusion of additional capabilities from its equipment manufacturer, ComNet can {[

]}[531] The PSI Report also recognized how the Companies work closely with their indirect parent, CITIC Tel, stating that ComNet "leverages [CITIC Tel's] network operations center (NOC), located in Hong Kong, for 'first tier monitoring' against cyber incidents or disruptions,"[532] and "used [CITIC Tel's] data center in Hong Kong as a backup."[533] We find that this integrated management

(Continued from previous page)

]}.

[528] ComNet is authorized under its international section 214 authorization, ITC-214-20090424-00199, to provide "*facilities-based and resale service* in accordance with section 63.18(e)(1) and (e)(2) of the Commission's rules . . . between the United States and all permissible foreign points, except China and Hong Kong." May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784 (emphasis added); May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. On the U.S.-China and U.S.-Hong Kong routes, ComNet is authorized to provide switched services solely through the resale of unaffiliated U.S. facilities-based carriers' international switched services (either directly or indirectly through the resale of another U.S. resale carrier's international switched services) pursuant to section 63.18(e)(3). May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. {[

]} PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-17; PN/CN June 1, 2020 Response at 13, 16; PN/CN April 28, 2021 Reply at 56-62; *see* May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. {[
]}

[529] PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-17. Additionally, {[

]} PN/CN April 28, 2021 Reply, Business Confidential Exh. D at D-17; *id*. at 56-62.

[530] *See* PN/CN June 1, 2020 Response, Business Confidential Exh. D at D-2 ({[ ]}).

[531] *See supra* para. 93; PN/CN June 1, 2020 Response, Business Confidential Exh. D at D-3, ({[ ]}). Our examination of the vendor documentation confirms this assessment. *See* {[

]} *See infra* para. 94 (explaining how VoIP technology is used by ComNet to support Wholesale IDD service).

[532] PSI Report at 96; PN/CN April 28, 2021 Reply at 65. The Companies state that "[t]he alleged discrepancies related to management are statements related to (i) involvement in daily operations, (ii) guidance of information security policies and (iii) monitoring provided by CITIC Tel's Hong Kong Service Operations Center ('SOC'), referred to as a 'NOC' in the PSI Report." *Id*.

[533] PSI Report at 96; PN/CN April 28, 2021 Reply at 65.

of network operations, {[ ]} and the fact that ComNet manages access to U.S. customer records by "coordinat[ing]" with CITIC Tel, as discussed above, present opportunities for ComNet, other entities in the Companies' ownership chain, and ultimately the Chinese government to obtain unauthorized access to CDRs and other sensitive information, both from within the United States {[ ]} which in turn presents an unacceptable risk.[534]

99. Further, we find that ComNet's operation of {[ ]} to provide its Wholesale IDD service as well as its non-section 214 VoIP service, raises additional national security and law enforcement concerns related to the potential for misrouting of communications.[535] We find that the inventory of equipment that the Companies identified for ComNet shows the use of {[

]}[542]

100. Specifically, given the functional capabilities of {[

[534] *See supra* paras. 84-87.

[535] See PN/CN June 1, 2020 Response, Business Confidential Exh. K at 24 ({[ ]}).

[536] *See id*., Business Confidential Exh. D at D-3 ({[ ]}).

[537] {[

]}

[538] *See supra* note 537.

[539] *See id.*

[540] {[

]}

[541] {[ ]}

[542] *See id*.

]} Accordingly, ComNet's operation of {[ ]} within the United States, combined with the Companies' majority ownership and control by the Chinese government, represents a threat to U.S. national security and law enforcement interests.

101. *Security Concerns Related to Physical Presence in the United States and Least-Cost Routing and Misrouting with Wholesale IDD Service.* The Executive Branch agencies raise concerns related to the security of least-cost routing. Specifically, the Executive Branch agencies observe that, "due to least-cost routing, the communications of U.S. government agencies to any international destinations may conceivably pass through the Companies' network during transit, even if the agencies are not actual customers of the Companies."[543] As described above, the national security and law enforcement risks associated with least-cost routing in the case of the Companies are that an upstream carrier may choose to send its traffic through ComNet's network, due to its physical location and availability, which then forwards the traffic towards the destination.[544] This is not the same as BGP routing, which also presents the potential for misrouting due to physical location;[545] rather, least-cost routing flows from decisions made at the application layer by another provider, which, because it reflects the least-cost option, results in traffic that is sent to and can be accessed and monitored by ComNet. In short, under operating arrangements maintained by the Companies, ComNet can take advantage of routing decisions by other carriers to access, monitor, and/or store data without authorization, even though it is not in a position to misroute traffic.[546] This opportunity for ComNet to engage in such activities presents significant risks to the national security and law enforcement interests of the United States.

102. *Voice over Internet Protocol (VoIP)/Non-Section 214 Service.* The Companies state that ComNet "serves as a VoIP service provider through a cloud-based PBX platform to enterprise users that offers the functions of an office telephone system without the need for the customer hosting a physical PBX in the office."[547] Customers of this service can make both national and international calls to numbers on the Public Switched Telecommunications Network (PSTN).[548] The Companies explain that "[e]ach VoIP phone used with the service is registered using a username and strong password protection on ComNet's VoIP Soft Switch located in ComNet's Los Angeles data center."[549] With regard to network routing, the Companies state that "ComNet takes outgoing calls and routes them only to an outgoing trunk connected to ComNet's wholesale voice switch, then uses SIP trunks to route to the ultimate

[543] Executive Branch Nov. 16, 2020 Letter at 10.

[544] *See supra* paras. 79, 100.

[545] *See supra* para. 80 (describing BGP routing).

[546] The Companies refer to comments filed by the Internet Governance Project at Georgia Tech University in a separate docket. The Companies observe that the Internet Governance Project, in that proceeding, asked whether misrouting is considered malicious hijacking, or whether these two acts should be distinguished. Those comments focused on BGP routing–and the potential for accidental or intentional misrouting using BGP–which is not at issue here. *See* PN/CN April 28, 2021 Reply at 39 (citing Internet Governance Project Comments, GN Docket No. 20-109; Internet Governance Project *Ex Parte* Comments, GN Docket No. 20-109). Our concerns about least-cost routing are distinct from the possibility of misrouting through the use of BGP. Thus, we reject the Companies' claim that there is a material question of fact based on assertions by the Internet Governance Project that the Commission should consider whether there is a need to distinguish between misrouting and malicious hijacking. *See supra* para. 34.

[547] PN/CN April 28, 2021 Reply at 57.

[548] *See id*. at 82-83.

[549] *Id*. at 83.

destination."[550] In their response to the *Institution Order*, the Companies include a "Diagram for ComNet VoIP Service" that provides more details on the provisioning of this service, including {[ ]}[551] and state that ComNet has {[ ]} customers for its VoIP service.[552]

103. Significantly, ComNet's provision of a related non-section 214 service, VoIP service, presents risks associated with ComNet's ability to access, monitor, store, and disrupt and/or misroute communications. Given that ComNet provides Wholesale IDD service using VoIP technology, as described above, the risks associated with ComNet's provision of VoIP service to enterprise customers are similar to the risks associated with its provision of Wholesale IDD service to customers.[553] Specifically, in its provision of VoIP service, ComNet uses equipment that includes {[ ]}[554] As discussed above, {[

]}
Moreover, with the inclusion of additional capabilities from its equipment manufacturer, ComNet can {[ ]}[556]
Although ComNet does not provide VoIP service pursuant to its section 214 authority, ComNet's provision of this service presents similar risks as those associated with ComNet's provision of Wholesale IDD service pursuant to its section 214 authority. Importantly, these services could be marketed collectively to potentially increase ComNet's appeal to even more customers.[557]

104. *Wholesale Short Message Service (SMS)/Non-Section 214 Service.* The Companies state that ComNet provides "international Short Message Service ('SMS') to carriers located in the U.S. and in foreign locations for delivering and receiving text messages between U.S. locations and rest of the world."[558] ComNet's provision of SMS includes the Application-to-Person (A2P) service that can be used

[550] *Id.*

[551] *Id*., Business Confidential Exh. I at I-2.

[552] *Id*., Business Confidential Exh. H at H-2.

[553] *See supra* paras. 94-100.

[554] *See* PN/CN June 1, 2020 Response, Business Confidential Exh. D at D-3 {[

]}

[555] *See supra* para. 99.

[556] *See* PN/CN June 1, 2020 Response, Business Confidential Exh. D at D-2 ({[

]})

[557] *See supra* para. 78 & note 438 (noting the variety of services provided by the Companies and the potential for these services to be marketed collectively).

[558] PN/CN June 1, 2020 Response at 14.

for notifications, to send Personal Identification Number (PIN) codes, and for two-factor authentication.[559] The Companies state that ComNet's provision of SMS "do[es] not require significant domestic communications facilities within the U.S."[560] In their response to the Commission's request that the Companies distinguish between A2P SMS messages that are sent through IP-based networks versus SS7, the Companies state that {[ ]}% of ComNet's A2P SMS messages use IP-based networks.[561] In their filing, the Companies further report that ComNet has {[ ]} customers for its Wholesale SMS, including {[ ]}[562]

105. ComNet's provision of a related non-section 214 service, SMS, presents risks associated with ComNet's ability to access, monitor, store, and/or disrupt communications. Like any similarly situated provider that offers SMS, ComNet is able to deploy message filtering as a means to protect customers from unwanted spam and attempts at fraud, and to prevent the delivery of abusive messages.[563] This capability can also be used for censorship at the discretion of the provider, or it can be used for storing data that clients consider personal and sensitive.[564] Whether the provider takes such actions to protect the customer or to exploit access to the customer (e.g., for purposes of espionage), in either case, the provider is capable of implementing such filtering actions without the knowledge of the customer. Additionally, the A2P service provided by ComNet can include one-direction messaging for notifications, PIN codes, and two-factor authentication, posing potential risks should the security of such information be compromised.[565] In particular, PINs and two-factor authentication codes involve sensitive customer information, and any exploitation of such information raises significant national security and law enforcement concerns. As with its provision of other services, ComNet sits at a privileged position as a provider of SMS, as it has the ability to access, monitor, store and/or in some cases disrupt customer communications. As with prepaid mobile SIM cards and VoIP service, ComNet can combine its section 214 service with the provision of its non-section 214 SMS service, thereby enhancing ComNet's ability to attract customers. As described above, ComNet's provision of these services raises significant national security and law enforcement risks.

106. *Multi-Protocol Label Switching Virtual Private Networks (MPLS VPN).* The Companies explain that "Pacific Networks' MPLS VPN service provides data communications that enable its customers to operate business applications among various customer sites both within the United States

[559] *See* PN/CN April 28, 2021 Reply at 73. For a description of A2P, *see What Is A2P Messaging?*, Arelion, https://www.arelion.com/knowledge-hub/what-is-guides/what-is-a2p-messaging html (last visited Mar. 11, 2022) ("Application-to-Person (A2P) messaging is one-direction messaging from an application to a person where no reply is expected.").

[560] PN/CN April 28, 2021 Reply at 58.

[561] *Id*. at 73 ("In 2020, {[ ]} % of A2P SMS connections used IP based networks."); *Institution Order*, 36 FCC Rcd at 6416, Appx. A.

[562] PN/CN June 1, 2020 Response, Business Confidential Exh. E at E-3. {[

]}

[563] *See* How To Avoid SMS Carrier Filtering, heyMarket, https://www.heymarket.com/blog/how-to/how-to-avoid-sms-carrier-filtering/ (last visited Mar. 13, 2022) (stating that one reason that carriers will use an SMS filtering system is to protect mobile users).

[564] We agree with other experts that this capability can be misused. *See* Chris Hoffman, *Why SMS Text Messages Aren't Private or Secure*, How-to Geek (Jan. 21, 2021), https://www howtogeek.com/709373/why-sms-text-messages-arent-private-or-secure/.

[565] *See* What Is A2P Messaging, *supra* note 559 (explaining that A2P is used for one-direction communications, with messages sent by an application to a person, such as an enterprise sending a text message to a customer or group of customers).

and internationally."[566] Pacific Networks' platform for the MPLS VPN service is located in two data centers, in New York and in Los Angeles, California, and Pacific Networks "purchases {[ ]}[567] The Companies explain that Pacific Networks leases {[ ]} for sublease to {[ ]}[568] The Companies state that Pacific Networks "does not, however, provide any services over these circuits, have access to the traffic carried over the circuits, and they are not connected to Pacific Network's [sic] points of presence or other locations."[569] To establish its connections within the United States, the Companies add that Pacific Networks "purchases from U.S. telecommunications carriers high-speed data connections to customer locations to facilitate provision of the service."[570] To establish its international connections, the Companies state that Pacific Networks "does not provide the international circuits required for international MPLS VPN—those facilities are purchased from unaffiliated international carriers by Pacific Networks' wholesale customer . . . and then interconnected with Pacific Networks' VPN platform in the United States . . . ."[571] In addition, the Companies state that "Pacific Networks has deployed [AS] number 4058 for its MPLS VPN platform in its New York and Los Angeles data centers" and, significantly, "[t]his [AS] number is assigned to {[ ]} not to Pacific Networks.[572]

107. With regard to access to U.S. customer records and customer support for the MPLS VPN service, the Companies state that "individuals employed by {[ ]}, a subsidiary of [CITIC Tel], have access to U.S. customer records to provide support and billing" and that {[ ]} provides first tier support for Pacific Networks' MPLS VPN service."[573] The Companies also state that "[b]oth of these services are provided to Pacific Networks pursuant to a services contract with {[ ]}, a subsidiary of {[ ]} a copy of which is attached hereto as Exhibit J."[574] As an initial matter, we observe that the services contract {[

[566] PN/CN June 1, 2020 Response at 12.

[567] PN/CN April 28, 2021 Reply at 58.

[568] *Id*.; PN/CN June 1, 2020 Response, Business Confidential Exh. E at E-1.

[569] PN/CN April 28, 2021 Reply at 58.

[570] PN/CN June 1, 2020 Response at 12-13.

[571] *Id*. at 12.

[572] PN/CN April 28, 2021 Reply at 61. *See supra* note 269 ({[ ]}).

[573] PN/CN April 28, 2021 Reply at 72. While service providers vary in terms of what they offer for "first tier support," this is generally considered to be the first level of support provided to the customer, to help with a variety of common user problems. *See* Chrissy Kidd & Joe Hertvik, *IT Support Levels Clearly Explained: L1, L2, L3 & More*, BMC Software Blogs (Apr. 25, 2019), https://www.bmc.com/blogs/support-levels-level-1-level-2-level-3/; *What Is Level 1, Level 2, And Level 3 IT Support?*, NetEffect (Aug. 17, 2020), https://neteffect.com/level-1-2-3-support/ ("The technicians in Level 1: Collect customer requests and data; Attend to customer phone calls; Respond to user emails and social media messages; Conduct basic troubleshooting using questionnaires to find out the level of support needed; Create tickets for Level 2 support; Provide product information; Solve common problems such as username and passwords issues, menu navigation, verification of hardware and software, installation issues, and setup.").

[574] PN/CN April 28, 2021 Reply at 72; *but see id.* at 49 (responding specifically to the Commission's inquiry involving access to U.S. customer records by stating, {[

(continued….)

]}[576] In fact, the services contract states that {[

]}[579]

108. We find that there are serious and significant national security and law enforcement risks associated with Pacific Networks' provision of MPLS VPN service offered pursuant to its international

(Continued from previous page)

]}). According to the Companies, "[n]either of these subsidiaries is a direct or indirect owner of either of the Companies. They are thus affiliates, not owners, of Pacific Networks." *Id.*

[575] *See id*., Business Confidential Exh. J at J-2 ({[

]}).

[576] *See generally id*., Business Confidential Exh. J.

[577] *Id*., Business Confidential Exh. J at J-2.

[578] *Id*. The services agreement states that {[

]} *Id*. at J-2-J-3 (emphasis added).

[579] PN/CN April 28, 2021 Reply, Business Confidential Exh. J at J-2-J-3. In describing Pacific Networks' domestic communications and its connectivity to operations infrastructure to Hong Kong, the Companies describe the circuits Pacific Networks leases to provide service and notes that "Pacific Networks does not, however, provide any services over these circuits, have access to the traffic carried over the circuits, and they are not connected to Pacific Network's [sic] points of presence or other locations." *Id*. at 58.

section 214 authority.[580] Based on the Companies' description of the arrangement involving Pacific Networks' MPLS VPN service and the services contract, {[

]}[581] Pursuant to this services contract, both Pacific Networks and {[
]}[582] Specifically, Pacific Networks {[

[580] Pacific Networks is authorized under its international section 214 authorization, ITC-214-20090105-00006, "to provide *resale* service in accordance with section 63.18(e)(2) on all U.S. international routes, except U.S.-China and U.S.-Hong Kong." April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384 (emphasis added). On the U.S.-China and U.S.-Hong Kong routes, Pacific Networks is authorized to provide switched services solely through the resale of unaffiliated U.S. facilities-based carriers' international switched services (either directly or indirectly through the resale of another U.S. resale carrier's international switched services) pursuant to section 63.18(e)(3). *Id*.

[581] *See supra* para. 106; PN/CN April 28, 2021 Reply at 72; *id.*, Business Confidential Exh. J at J-2 ({[

]}). The MPLS VPN service offering by Pacific Networks involves switched services, or what the industry has construed to be switched services using labels. We agree with the Companies' explanation that, "[w]hile Pacific Networks' MPLS VPN does use BGP routers, the service is *not* an IP Transit service." PN/CN April 28, 2021 Reply at 61. As the Companies stated in their response to the *Order to Show Cause*, "Pacific Networks' MPLS VPN service provides data communications between and among customer sites within the U.S., and internationally, enabling the operation of business applications at those sites. The service does not provide IP Transit for Internet service." *Id.*; *see* PN/CN June 1, 2020 Response at 12. At the same time, MPLS, by design, involves an element of switched service in its architecture, and the word "switching" comprises part of its name, "Multi-Protocol Label Switching." Accordingly, we consider Pacific Networks' provision of MPLS VPN service to be a switched service. *See also* PN/CN April 28, 2021 Reply at 55-56 (stating that the Companies consider the MPLS VPN service to be provided pursuant to Pacific Networks' section 214 authorization); Richard A. Steenbergen, *MPLS for Dummies*, North American Network Operators Group (NANOG) Archives 7-8, https://archive.nanog.org/sites/default/files/tuesday_tutorial_steenbergen_mpls_46.pdf (last visited Mar. 13, 2022); Cisco, *Multiprotocol Label Switching (MPLS) Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst 3850 Switches)* (Jan. 8, 2019), https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-6/configuration_guide/mpls/b_166_mpls_3850_cg/b_166_mpls_3850_cg_chapter_00.html (referring to MPLS "switches"). {[

]} *See supra* note 583; April 28, 2021 Reply, Business Confidential Exh. D at D-18, D-20; June 1, 2020 Response at 12-13; *see* April 28, 2021 Reply at 56-62; April 9, 2009 Grant Public Notice, 24 FCC Rcd at 4156; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. {[

]}
See infra paras. 109-112.

[582] PN/CN April 28, 2021 Reply, Business Confidential Exh. J at J-2, J-3 ({[

]}); *id.,* Business Confidential Exh. J at J-4 ({[

(continued….)

]}[583] In addition, based on the Companies' admission, {[ ]} has access to U.S. customer records to provide support and billing and {[ ]} provides first tier customer service support for Pacific Networks' MPLS VPN service.[584] Similar to our concerns above, {[ ]} have access to PII, CPNI, and/or metadata, along with the opportunity to use this information contrary to U.S. interests.[585]

109. We also find that {[ ]} manage necessary elements of Pacific Networks' MPLS VPN service. As stated above, Pacific Networks deploys the AS number of {[ ]} to support the MPLS VPN platform.[586] This AS peers[587] (i.e., directly interconnects) with multiple transit provider networks that in turn peer with Chinese provider networks.[588] We note that an AS number is associated with a set of IP addresses, which means that these IP addresses are associated with {[ ]}[589] and are used to support the VPN part of Pacific Networks' MPLS VPN service. The provisioning of MPLS VPN service requires: (1) an IP address for each customer's computer; (2) an AS number and set of IP addresses from the provider of the MPLS VPN service; and (3) an MPLS network within the provider's network. Based on the record evidence, {[ ]} therefore have the ability to access, monitor, store, and/or disrupt Pacific Networks' customer VPN traffic. Further, as

(Continued from previous page)

]}).

[583] PN/CN April 28, 2021 Reply, Business Confidential Exh. J; *id.* at 72; *see supra* notes 581, 582.

[584] PN/CN April 28, 2021 Reply at 72; *see id.*, Business Confidential Exh. J; *id.* at 49-50.

[585] *See Guide to Protecting the Confidentiality of Personally Identifiable Information*, *supra* note 484 (discussing harms related to access to PII); *A Look at What ISPs Know About You*, *supra* note 501 (discussing harms related to ISPs' access to PII and to metadata); IETF, *Request for Comments: 6071, Category: Informational, IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*, *supra* note 506 (discussing harms related to monitoring).

[586] *See* American Registry for Internet Numbers (ARIN), *What Are Autonomous System Numbers?*, https://www.arin.net/resources/guide/asn/ (last visited Mar. 13, 2022).

[587] *See Peering Policy—Peering Policy Overview and Technical Requirements*, ThousandEyes, https://www.thousandeyes.com/learning/techtorials/peering-policy (last visited Mar. 13, 2022) (explaining peering requirements and policies, which are criteria to determine the networks with which an ISP interconnects or peers with other ISPs, and their use by network operators, including BGP routing). We note that while the Companies provide a copy of the contract between Pacific Networks and {[ ]} the Companies have not provided a copy of any contract that describes {[ ]} Further, the Companies have not provided a copy of any contract or arrangement that describes {[ ]}

[588] *See* Hurricane Electric Internet Services, *IPv4 Peers of AS-4058*, https://bgp.he.net/AS4058#_peers (last visited Mar. 14, 2022); Hurricane Electric Internet Services, *IPv4 Peers of AS-10099,* https://bgp he net/AS10099#_peers (last visited Mar. 14, 2022) (noting that AS-10099 peers with China Netcom Backbone and China Unicom Backbone).

[589] *See* Hurricane Electric Internet Services, *IPv4 IP address assignments for AS-4058*, *supra* note 515. All but one set of IP addresses are assigned by the Asia Pacific Network Information Centre (APNIC).

explained above, even if traffic is encrypted end-to-end, {[ ]} can derive metadata[590] from this traffic and attempt to decrypt client-encrypted traffic to access the content at a time and location of their choosing.[591]

110. In addition, {[ ]} could leverage Pacific Networks' physical presence in the United States, as well as Pacific Networks' network connection to other providers in the United States, which in turn could facilitate {[ ]} access to data in the underlying communications through future peering agreements.[592] While we recognize that Pacific Networks' physical operations are limited to Los Angeles, California and New York, these operations provide Pacific Networks' {[ ]} with important access to such data.

111. We note that every network service provider "sits at a privileged place in the network . . . from which it enjoys the ability to see at least part of every single packet sent to and received from the rest of the Internet."[593] Individuals, companies, and others using the Companies' services entrust their data and communications to the Companies. It is critical that a network service provider understand the significance of this trusted role. As explained in historic English common law jurisprudence, anyone entrusted with possession of property owned by another has "an opportunity of undoing all persons who have had dealings with them," by engaging in malicious activity "and yet doing so in a clandestine manner, as would not be possible to be discovered."[594] Therefore, trusted relationships with service providers remain critical today.[595] While Pacific Networks {[

[590] We agree with other experts who have identified concerns about the ways this capability can be used for illicit purposes. *See* Joseph Cox, *How Data Brokers Sell Access to the Backbone of the Internet*, Vice (Aug. 24, 2021), https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru (noting how ISPs can trace traffic through virtual private networks). *See also* European Union Agency for Cybersecurity (ENISA), *Encrypted Traffic Analysis: Use Cases & Security Challenges* 7 (Nov. 2019), https://www.enisa.europa.eu/publications/encrypted-traffic-analysis (stating, "The privacy of Internet users is therefore largely threatened by encrypted traffic analysis . . . "). We agree with both analyses that the use of encryption does not prevent the Companies from discovering information about customer traffic and using it for illicit purposes.

[591] *See supra* para. 93.

[592] Pacific Networks can use its physical infrastructure to enter into future peering agreements with other networks.

[593] Letter from Paul Ohm, Professor, Georgetown University Law Center, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106 Attach. at 3 (filed June 19, 2016) (Statement of Paul Ohm, Professor, Georgetown University Law Center and Faculty Director, Georgetown Center on Privacy and Technology Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives (June 14, 2016)) (Paul Ohm Statement); *see NIST Guide to Intrusion Detection and Prevention Systems*, *supra* note 501 (discussing Deep Packet Inspection).

[594] *Coggs v. Bernard*, (1703) 2 Ld Raym 909, 918, 92 ER 107 (articulating the historic concern of vulnerability of customers who entrust goods to common carriers); *China Telecom Americas Order on Revocation and Termination* at *34, n.403; *China Unicom Americas Order on Revocation*, FCC 22-9 at n.464. Communications law has historically recognized the unique trust relationship between customers and network service providers, and their vulnerability to bad acts by providers. *See NARUC I*, 525 F.2d at 640-41 (describing a historical rationale for the treatment of common carriage as "the lack of control exercised by shippers or travellers over the safety of their carriage," and describing the relationship of the carrier to its customers as one of "public trust"). *See also* Barbara Cherry, The Crisis in Telecommunications Carrier Liability: Historical Regulatory Flaws and Recommended Reform 12 (1999) ("*Coggs v. Bernard* is considered the case on which the modern law of bailees is based."); Oliver Wendell Holmes, The Common Law, Lecture V: The Bailee at Common Law 164 (1881); Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), https://go.usa.gov/xtYGu (discussing users' lack of trust in the security of their data and communications on the Internet).

[595] *See* Paul Ohm Statement at 3; Harold Feld, et. al., *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World*, Public Knowledge (2016), (continued….)

]}[596] and Pacific Networks, {[ ]} nevertheless retain the opportunity to engage in the harmful activities described above.[597] Importantly, Pacific Networks provides the means (e.g., physical network infrastructure, as well as section 214 authority, to provide MPLS VPN service) by which these {[ ]} may conduct those harmful activities. Pacific Networks thus has significant opportunity to enable and facilitate both active attacks and passive or pervasive monitoring given that {[ ]} that in turn can be exploited for such activities, maintains the physical network infrastructure for the provision of services in the United States, and holds the section 214 authority to provide the MPLS VPN service.

112. *Security Concerns Related to Physical Presence in the United States and the Ability to Combine Pacific Networks' MPLS VPN Service with ComNet's Services.* The physical location of the Companies' operations with respect to their points of presence in the United States is relevant to these identified national security and law enforcement risks. These concerns are distinguished from concerns pertaining to network (rather than application) routing by a provider, such as accidental or intentional misrouting related to BGP, a concern that is influenced by physical location.[598] Rather, the concerns about the Companies' physical presence relates to Pacific Networks' MPLS VPN service and Pacific Networks' current and potential physical connectivity to other networks in the United States. The Companies state that Pacific Networks "maintains various physical points of interconnection with unaffiliated carriers to provide the international circuits used by its MPLS VPN customers for communication with customer sites located outside the U.S."[599] However, as discussed above, the Companies have disclosed that {[ ]} provides the AS number used for the VPN platform, which implies that IP plays a role in some form in supporting the MPLS VPN service. As indicated above, Pacific Networks, as ComNet's direct parent entity, may combine its MPLS VPN service with ComNet's section 214 and non-section 214 services, thereby enhancing Pacific Networks' ability to attract customers.

113. We find that ComNet's and Pacific Networks' provision of the services described above—Retail Calling Card, Wholesale IDD, and MPLS VPN services—presents significant national security and law enforcement risks to the United States. These services, offered individually or with other related non-section 214 services, when combined with the Companies' physical presence in the United States, their interconnection with other service providers,[600] their majority ownership and control by the Chinese government, their relationship with their parent entities and affiliates, and their vulnerability to exploitation, influence, and control by the Chinese government,[601] present unacceptable national security and law enforcement risks to the United States requiring revocation of the Companies' section 214 authority.

(Continued from previous page)
https://publicknowledge.org/policy/protecting-privacy-promoting-competition-white-paper/ (discussing the data that can be gathered by a network service provider from its customers and end users).

[596] PN/CN April 28, 2021 Reply, Business Confidential Exh. J at J-2.

[597] *See supra* paras. 108-110.

[598] *See* PN/CN April 28, 2021 Reply at 62 ("Pacific Networks does not have any peering relationships with U.S. providers for the exchange of Internet traffic, since it only provides MPLS VPN service to its customers and does not peer with other providers for the exchange of Internet traffic, as explained in response to Question 16.").

[599] PN/CN April 28, 2021 Reply at 62-63.

[600] *See supra* para. 110.

[601] *See supra* Section III.B.1.

3. The Companies' Past Conduct and Representations to the Commission and Congress Require Revocation of Their Section 214 Authority

114. The Companies' past representations to the Commission and Congress require us to find—independent of our separate concerns about the intent and ability of the Chinese government to use its influence and control over the Companies in ways that pose serious risks to critical U.S. national security and law enforcement interests—that the public interest, convenience, and necessity is no longer served by the Companies' retention of their section 214 authority. Thus, these concerns present a separate and independent basis for revoking the Companies' section 214 authority. We find that the Companies failed to fully respond to several questions in the *Order to Show Cause* and the *Institution Order* concerning their ownership and control.[602] Among other things, the Companies failed to provide the Commission with highly relevant information that they provided to the Senate Subcommittee and that was disclosed in the PSI Report concerning the extent of the involvement and control of their indirect parent corporation, CITIC Tel, which would have been directly responsive to the questions in the *Order to Show Cause*.[603] The Companies failed to comply with the Commission's *pro forma* notification rules when they failed to file *pro forma* notifications of a 2014 restructuring for approximately seven years and a *pro forma* notification concerning a change in the Companies' ultimate majority ownership from SASAC to the Ministry of Finance for over ten years. In the event that the Ministry of Finance was always the government entity that majority-owned and controlled the Companies, the Companies provided the Commission with inaccurate information in multiple filings,[604] and had several opportunities to rectify the record throughout the pendency of these proceedings, but failed to do so.

115. The Companies' transparency and truthfulness with the Commission and the U.S. government generally, as well as their ability to comply with the Commission's rules, are essential characteristics to demonstrate that the Companies' retention of their section 214 authority continues to serve the public interest, convenience, and necessity.[605] As stated above, trust is paramount given that carriers sit at a privileged position to provide critical telecommunications services in the United States.[606] Although the Companies had several opportunities to do so, the Companies provided no additional persuasive evidence in the record to dispel the concerns that were identified in the *Institution Order*.[607] We find that the inadequacies in the Companies' representations to the Commission and Congress demonstrate the Companies' lack of transparency and reliability as well as their failure to comply with the Commission's rules.[608] Based on the record evidence, we find that the Companies cannot be trusted to cooperate with the Commission or the Executive Branch agencies, to comply with the Commission's rules, and, importantly, to assist with the Commission's statutory obligations to act "for the purpose of the national defense [and] for the purpose of promoting safety of life and property."[609]

---

[602] *Order to Show* Cause, 35 FCC Rcd at 3737-39, paras. 8-10; *Institution Order*, 36 FCC Rcd at 6415-17, Appx. A.

[603] *See* PSI Report at 95-96; *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[604] *See Institution Order*, 36 FCC Rcd at 6372-73, para. 5 ("According to Commission records, the State-owned Assets Supervision and Administration Commission of the State Council, a Chinese government organization, directly owns 100% of CITIC Group Corporation. Other publicly available information, however, indicates that CITIC Group Corporation is funded and owned by China's Ministry of Finance."); 47 CFR § 1.65; *see also infra* paras. 121-123.

[605] *Institution Order*, 36 FCC Rcd at 6404, para. 52.

[606] *See supra* para. 111.

[607] *See Institution Order*, 36 FCC Rcd at 6404-09, paras. 52-61.

[608] *See id*.

[609] Congress created the Commission, among other reasons, "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications . . . ." 47 USC § 151.

a. Failure to Fully and Accurately Respond to the *Order to Show Cause* and the *Institution Order* and Comply with Commission Rules

116. The record is clear that the Companies failed to fully and accurately respond to the *Order to Show Cause* and the *Institution Order*, and based on our review of the Companies' responses in this matter, the Companies also failed to comply with the Commission's rules. We find that the Companies' repeated omission of crucial information that was directly responsive to the directives in those Orders, combined with the Companies' failure to comply with our rules, affirms our concerns regarding the Companies' lack of transparency, trustworthiness, and reliability. Specifically, the Companies failed to: (1) identify all of their 10% or greater interest holders; (2) identify the Chinese government entity with majority ownership and control, as required by the Commission's rules; (3) provide information on the extent of control and involvement of CITIC Tel as well as the role of {[ ]} another subsidiary of CITIC Tel, in the Companies' management and operations; (4) provide information concerning the location of and access to certain U.S. records; and (5) timely file *pro forma* notifications concerning the 2014 corporate restructuring.[610]

117. *Ten-Percent-or-Greater Interest Holders.* The Companies' failure to fully respond to basic and fundamental questions concerning the identity of individuals that comprise the corporate leadership of entities holding a 10% or greater direct or indirect interest in the Companies undermines our confidence in the Companies' ability to work cooperatively with the Commission and comply with our rules. The *Order to Show Cause* directed the Companies to provide "an identification of all officers, directors, and other senior management officials of entities that hold [10%] or greater ownership interest in Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government."[611] The Companies, in their response, provided information only for Pacific Networks' direct parent, Pacific Choice International Limited,[612] even though their response indicated the existence of other entities in the Companies' vertical chain of ownership that hold 10% or greater ownership interest in the Companies.[613]

118. We discussed this discrepancy in the *Institution Order* and directed the Companies to provide "an identification of all officers, directors, and other senior management of all entities that hold a [10%] or greater *direct or indirect* ownership interest in and/or control Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government."[614] We further noted in the *Institution Order* that "the Companies' failure to fully respond to the *Order to Show Cause*, or provide documentation of or citations to the 'respective website' of the two identified entities out of the 'numerous' entities in their ownership structure, or certify that the information on the 'respective websites' is responsive to the directive in the *Order to Show Cause*, raises troubling questions about their transparency and reliability."[615]

119. The Companies again failed to fully respond to our directive in the *Institution Order*.[616] Instead of providing the requisite information for all entities with 10% or greater ownership interest in the

[610] *See* PSI Report at 95-96; *Institution Order*, 36 FCC Rcd at 6405-06, paras. 55-56.

[611] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[612] *Institution Order*, 36 FCC Rcd at 6407-08, para. 58.

[613] *See* PN/CN June 1, 2020 Response, Exh. A (Pacific Networks & ComNet Organization Chart as of May 28, 2020).

[614] *Institution Order*, 36 FCC Rcd at 6415, Appx. A (emphasis added).

[615] *Id.* at 6408, n.277.

[616] *See supra* notes 29-31; PN/CN June 1, 2020 Response, Exh. A (Pacific Networks & ComNet Organization Chart as of May 28, 2020).

Companies, the Companies provided information for only three entities—CITIC Tel, CITIC Limited, and CITIC Corporation Group—by providing weblinks to the websites of those three entities.[617] The Companies failed to provide information concerning more than 10 entities that hold a 10% or greater ownership interest in the Companies.[618] Moreover, in directing the Commission to obtain information pertaining to CITIC Tel, CITIC Limited, and CITIC Group Corporation from these entities' webpages, the Companies failed to certify the accuracy and completeness of the information on the webpages.[619] Notably, the Companies did not acknowledge whether the information contained in each of these entities' webpages includes "*all* officers, directors, and senior management"[620] of each entity or whether the information on the webpages fully and accurately addresses the employment history (including prior employment with the Chinese government) and any affiliations with the Chinese Communist Party and

[617] PN/CN April 28, 2021 Reply at 45-46. In their response to this directive in the *Order to Show Cause*, the Companies stated that "the two public company entities in the ownership structure, CITIC Limited and CITIC Tel, are publicly traded companies listed on the Hong Kong Stock Exchange. As such, the identity of their respective senior management personnel is a matter of public record (and is listed on those companies' respective websites) . . . ." PN/CN June 1, 2020 Response at 12. In the *Institution Order*, we noted that "Pacific Networks and ComNet provided this information for only Pacific Choice International Limited, the direct parent of Pacific Networks," and instead of providing the requisite information for other entities that hold 10% or greater ownership interest, "Pacific Networks and ComNet direct the Commission to look at the public record." *Institution Order*, 36 FCC Rcd at 6408, para. 58. We stated that the Companies did not provide citations to the websites and that their "failure to fully respond to the *Order to Show Cause*, or provide documentation of or citations to the 'respective websites' of the two identified entities out of the 'numerous' entities in their ownership structure, or certify that the information on the 'respective websites' is responsive to the directive in the *Order to Show Cause*, raises troubling questions about their transparency and reliability." *Institution Order*, 36 FCC Rcd at 6408, n.277.

[618] The organizational chart in Exhibit A of the Companies' response to the *Order to Show Cause* shows the following entities in the Companies' vertical chain of ownership, as of May 28, 2020: (1) Pacific Choice International Limited holds 100% ownership interest in Pacific Networks; (2) four entities holding ownership interests in CITIC Tel, a publicly-traded entity on the Hong Kong Stock Exchange (Richtone Enterprises Inc. (3.68%), Ease Action Investments Corp. (33.89%), Perfect New Holdings Limited (3.87%), and Silver Log Holdings Ltd. (16.68%)); (3) Peganin Corp. holds 100% ownership interest in Richtone Enterprises Inc., Ferretti Holdings Corp. holds 100% ownership interest in Ease Action Investments Corp., All Achieve Investments Limited holds 100% ownership interest in Perfect New Holdings Limited, and CITIC Investment (HK) Limited holds 100% ownership interest in Silver Log Holdings Ltd.; (4) Douro Holdings Inc. holds 100% ownership interest in Peganin Corp., Ferretti Holdings Corp., and All Achieve Investments Limited; (5) CITIC Pacific Communications Limited holds 100% ownership interest in Douro Holdings Inc.; (6) Effectual Holdings Corp. Limited holds 100% ownership interest in CITIC Pacific Communications Limited; (7) Crown Base International Limited holds 100% ownership interest in Effectual Holdings Corp. Limited; (8) CITIC Pacific Limited holds 100% ownership interest in Crown Base International Limited; (9) CITIC Corporation Limited holds 100% ownership interest in CITIC Investment (HK) Limited; (10) CITIC Limited holds 100% ownership interest in CITIC Pacific Limited and CITIC Corporation Limited; (11) two entities holding ownership interests in CITIC Limited, publicly-traded entity on the Hong Kong Stock Exchange (CITIC Polaris Limited (32.53%) and CITIC Glory Limited (25.60%)); (11) CITIC Group Corporation holds 100% ownership interest in CITIC Polaris Limited and CITIC Glory Limited. PN/CN June 1, 2020 Response, Exh. A. The Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation. PN/CN April 28, 2021 Reply at 43.

[619] With regard to CITIC Tel, the Companies state, "[a] list of CITIC Tel's directors and corporate management, together with biographies for each of them, can be found at https://www.citictel.com/about-us/leadership/." PN/CN April 28, 2021 Reply at 45. With regard to CITIC Limited, the Companies state, "[a] list of CITIC Limited's directors, senior management and management, together with biographies for each of them, can be found at https://www.citic.com/en/aboutus/board_of_directors/, https://www.citic.com/en/aboutus/senior_management/ and https://www.citic.com/en/aboutus/management/." *Id.* at 45-46. With regard to CITIC Group Corporation, the Companies state, "[a] list of the members of CITIC Group's Group Party Committee, Board of Directors, Board of Supervisors, and Senior Management, together with biographies for each of them, can be found at https://www.group.citic/en/About_CITIC/Directors_Senior/." *Id*. at 46.

[620] *Institution Order*, 36 FCC Rcd at 6415, Appx. A.

the Chinese government of all officers, directors, and senior management of each entity—the information sought by both the *Order to Show Cause* and the *Institution Order*.[621] After examining the websites, we are unable to determine the completeness of the information contained therein. While the websites provide descriptions of employment history and, in the case of CITIC Group Corporation's website, certain information about the Chinese Communist Party affiliation of certain leadership components, the Companies do not state whether the websites reflect all material information associated with each identified individual, or whether any material information is omitted, including any current affiliations with the Chinese Communist Party and the Chinese government. Indeed, the webpage that the Companies associate with CITIC Tel does not affirmatively state whether or not the individuals identified on the webpage are associated with the Chinese Communist Party or the Chinese government.[622] Further, the webpages that the Companies associate with CITIC Limited do not contain information concerning the Chinese Communist Party affiliation of the company's corporate leaders that is, in contrast, reflected on CITIC Group Corporation's website with regard to certain of those individuals.[623] The Companies offer no such clarity or explanation in their response to the *Institution Order*.

120. The Companies' failure to provide complete responses to this directive is further evident based upon our review of the CITIC Tel Information Security Policy.[624] {[

[621] *See supra* para. 58. For instance, the Companies simply refer to the "biographies" on the webpages and do not affirmatively state whether the webpages associated with these three entities contain information about each corporate official's affiliations with the Chinese Communist Party or the Chinese government. With regard to CITIC Group Corporation, the Companies refer generally to "the members of CITIC Group's Group Party Committee," and offer no acknowledgement or explanation that the "Group Party Committee" is associated with the Chinese Communist Party. PN/CN April 28, 2021 Reply at 46.

[622] *See About Us—Leadership*, *supra* note 238. Furthermore, CITIC Tel's webpage states of the Chairman of CITIC Tel, "*[a]fter serving a substantial period of time in the government of the People's Republic of China (the 'PRC') in which Mr. Xin was involved in the administration of science, technology information and economics*, Mr. Xin joined in succession various major conglomerates as senior management, researcher or chief engineer. When Mr. Xin was with China Netcom (Hong Kong) Operations Limited, he held the position of Senior Vice President and Senior Consultant. *Mr. Xin had also participated in the planning, implementation and management of many different important state projects.*" *Id.* (emphasis added). CITIC Tel's webpage does not clarify, and the Companies do not explain, whether the Chairman of CITIC Tel continued to have affiliations with the Chinese government "after serving a substantial period of time in the government of the People's Republic of China" or currently has any affiliations with the Chinese government.

[623] *Compare CITIC Group Corporation—Board of Directors and Senior Managements, supra* note 243 (identifying Chinese Communist Party affiliation of corporate leadership, including the three Executive Directors, associated with the company's "Group Party Committee"), *with CITIC Limited Board of Directors*, *supra* note 309 (reflecting that CITIC Limited has identical Executive Directors as that of CITIC Group Corporation, yet not providing information about the Chinese Communist Party affiliation of at least two of the Executive Directors), *and CITIC Limited Senior Management*, *supra* note 243 (identifying six individuals as part of CITIC Limited's "Senior Management," and who are also part of CITIC Group Corporation's corporate leadership and Chinese Communist Party organization, yet not providing information about the Chinese Communist Party affiliation of at least five of the individuals).

[624] PN/CN April 28, 2021 Reply, Business Confidential Exh. B.

[625] *Id*., Business Confidential Exh. B at B-16

[626] *Id*.

]}[629] Notwithstanding these provisions in the CITIC Tel Information Security Policy, the Companies identified no such {[

]} despite the directives in the *Order to Show Cause* and the *Institution Order* that the Companies do so. Additionally, although the webpage that the Companies associate with CITIC Tel identifies certain members of CITIC Tel's corporate leadership,[630] it does not identify whether any of those individuals {[

]}[631]

121. *Ownership and Control by the Chinese Government/Failure to Comply with Commission's Rules*. We find that the Companies were not transparent and did not provide complete information regarding the Chinese government entity that has majority ownership and control of the Companies in their response to the *Order to Show Cause* and, based on our review of the Companies' responses, the Companies failed to comply with the Commission's rules. In the *Order to Show Cause*, based on the latest information from the Companies in the 2012 *pro forma* transfer of control notifications,[632] the Bureaus stated that "[SASAC], a Chinese government organization, directly owns 100% of CITIC Group Corporation."[633] In that Order, the Bureaus directed the Companies to provide "a detailed description of the current ownership and control (direct and indirect) of the companies and the place of organization of each entity in the ownership structure."[634] In their response to the *Order to Show Cause*, the Companies stated that "the ultimate parent entity of the licensees is state-owned CITIC Group Corporation,"[635] and failed to identify the government entity that owns CITIC Group Corporation and the entity's ownership interest in CITIC Group Corporation.[636] Additionally, the ownership chart that the

[627] *Id*., Business Confidential Exh. B at B-16-B-17.

[628] *Id*., Business Confidential Exh. B at B-17.

[629] *Id*.

[630] *About Us—Leadership*, *supra* note 238.

[631] *Id*. The CITIC Tel Information Security Policy provided in Exhibit B {[ ]} PN/CN April 28, 2021 Reply, Business Confidential Exh. B at B-2. The Companies refer to this document as "the current version of the CITIC Tel Information Security Policy." *Id.* at 48. Based on the record, we thus understand that the information contained in {[ ]} of the CITIC Tel Information Security Policy is current as of the Companies' April 28, 2021 filing with the Commission, and the Companies have not indicated otherwise. At the same time, the Companies failed to {[ ]} Additionally, CITIC Tel's webpage, to which the Companies cite, {[ ]} *See id.*, Business Confidential Exh. B at B-16-B-17.

[632] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[633] *Id.* at 3735, para. 4; *Institution Order*, 36 FCC Rcd at 6407, para. 57 ("In support of this statement, the Bureaus cited to *pro forma* transfer of control notifications that were filed on behalf of Pacific Networks and ComNet in 2012.").

[634] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[635] PN/CN June 1, 2020 Response at 33.

[636] *Id*. at 10.

Companies submitted as Exhibit A did not include the Chinese government (neither generally nor any specific governmental entity) or the percentage of the ownership interest held directly in CITIC Group Corporation, and held indirectly in the Companies, by the Chinese government.[637]

122. Subsequently, in the *Institution Order*, we described the discrepancy between the Companies' records on file with the Commission and other publicly available information regarding the ultimate owner of the Companies.[638] In particular, we indicated that the websites of the Companies' ultimate parent entity, CITIC Group Corporation, and an indirect parent entity, CITIC Limited, state that the Ministry of Finance, not SASAC, owns CITIC Group Corporation.[639] We also stated that the Ministry of Finance and SASAC appear to be different government entities with different leadership.[640] In the *Institution Order*, we directed the Companies "to clarify this ambiguity in their response to this Order."[641] We further directed the Companies to include in their response "an identification of the Chinese government entity that owns and controls CITIC Group Corporation and the ownership interests held by such entity in CITIC Group Corporation."[642] The Companies' response to the *Institution Order*, however, provided minimal information and stated without further explanation that "[t]he Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation,"[643] a perfunctory response that fails to explain the discrepancy in the Companies' previous filings with the Commission.[644]

---

[637] *Id*., Exh. A.

[638] *Institution Order*, 36 FCC Rcd at 6406-07, para. 57.

[639] *Id*.

[640] *Id.* (citing State-owned Assets Supervision and Administration Commission of the State Council, *About Us*, http://en.sasac.gov.cn/aboutus.html (last visited Mar. 1, 2022) (*SASAC About Us*); The State Council of the People's Republic of China, *Ministers*, http://english.www.gov.cn/statecouncil/202008/12/content_WS5f334b75c6d029c1c26379c3.html (last visited Mar. 1, 2022)).

[641] *Id.* at 6372-73, para. 5, n.20 (referring to Appx. A).

[642] *Id.* at 6415, Appx. A.

[643] PN/CN April 28, 2021 Reply at 43.

[644] 2012 Pacific Networks Pro Forma TC Notification, Attach. 1, Exh. A; 2012 Pacific Networks Pro Forma TC Notification, Attach. 1, Exh. A and Exh. B; *see* May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. Filings submitted by the Companies and their ultimate parent entity, CITIC Group Corporation, to different U.S. government agencies provide conflicting information regarding their ultimate majority ownership by the Chinese government. For instance, the Companies' filings with the Commission consistently identified SASAC as the Chinese government entity that directly owns CITIC Group Corporation, while CITIC Group Corporation's submissions to the FDIC, which are publicly available as of 2013, identified the Ministry of Finance as the "sole shareholder of [CITIC Group Corporation]." *See supra* note 28; CITIC Group Corporation, 2013 Tailored U.S. Resolution Plan (Public Section) at 6, https://www.fdic.gov/resources/resolutions/resolution-authority/resplans/plans/chinacitic-165-1312.pdf; *Institution Order,* 36 FCC Rcd at 6373, n. 20. Additionally, further research by the Commission shows that another subsidiary of CITIC Group Corporation has reported the Ministry of Finance to be the Chinese government entity that owns CITIC Group Corporation since at least the date of that entity's report in 2008. China CITIC Bank Corporation Limited, 2007 Annual Report at 111 (Apr. 30, 2008), https://www1.hkexnews hk/listedco/listconews/sehk/2008/0430/ltn20080430257.pdf (providing an illustration of the "shareholding structure" demonstrating that the Ministry of Finance is the direct shareholder of CITIC Group Corporation). This report predated the Companies' 2012 *pro forma* transfer of control notifications. Further, in 2009, the Ministry of Finance issued "Several Provisions on the Financial Management of Financial Holding Companies," which stated that "[t]he state-owned capital of financial holding companies shall be held by the Ministry of Finance on behalf of the state" and specifically identified CITIC Group Corporation as an entity to which the Provisions apply. Lawinfochina, *Notice of the Ministry of Finance on Issuing Several Provisions on the Financial Management of Financial Holding Companies* (Sept. 1, 2009),

(continued….)

123. Based on the Companies' response to the *Institution Order*, we find that the Companies failed to file *pro forma* transfer of control notifications concerning the change of the Companies' majority ownership from SASAC to the Ministry of Finance, as required by section 63.24(f) of the Commission's rules. Specifically, the Companies failed to file *pro forma* notifications with the Commission concerning the change in the Chinese government organization that directly holds 100% interest in CITIC Group Corporation.[645] The Commission's *pro forma* notification rules are intended to ensure accurate ownership information. Based on the Companies' filings with the Commission from 2007 to 2012, until the Companies responded to the *Institution Order*, the Commission and the public understood that SASAC held and continued to hold 100% of CITIC Group Corporation's equity interest.[646] The Companies' vague response to the *Institution Order*, despite the discrepancy between their prior filings with the Commission and other public records, offers no insight or transparency as to when or how such a change occurred in the Companies' ownership, nor any further insight into the role of the Ministry of Finance with regard to the Companies.[647] We find it unacceptable that the Companies failed to disclose this basic

(Continued from previous page)
http://www.lawinfochina.com/display.aspx?lib=law&id=7793&CGid= (stating, "[t]hese Provisions shall apply to the financial management activities of the China CITIC Group . . . .").

[645] *See supra* Section III.B.3; Pacific Networks Corp., Application for International Section 214 Authority, File No. ITC-214-20070907-00368, Attach. 2 at 4 (filed Sept. 7, 2007) (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); Pacific Networks Corp., Application for Transfer of Control of International Section 214 Authority, File No. ITC-T/C-20081219-00543, Attach. 1 at 7 (filed Dec. 19, 2008) (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); Pacific Networks 2009 Application for International Section 214 Authority, Attach. 2 at 6 (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); 2012 Pacific Networks Pro Forma TC Notification, Attach. 1, Exh. A (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); *id.*, Pacific Networks Feb. 16, 2012 Letter at 10 (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); 2012 ComNet Pro Forma TC Notification, Attach. 1, Exh. A (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[d]irectly owns 100% of CITIC Group"); *id.*, ComNet Feb. 16, 2012 Letter at 10 (identifying "Assets Supervision and Administration Commission of the State Council of China" as the Chinese government entity that "[o]wns 100% of CITIC Group"); PN/CN June 1, 2020 Response, Business Confidential Exh. K at 4-7 (providing to DHS and DOJ a copy of the 2012 *pro forma* notification filed with the Commission and subsequently providing corrected versions on February 16, 2012); PN/CN April 28, 2021 Reply at 77, Exh. G (attaching corrected February 16, 2012 versions of the 2012 *pro forma* notifications, which identify SASAC in the Companies' vertical line of ownership); *see* PN/CN June 1, 2020 Response, Business Confidential Exh. K at 12-16 (notifying DHS and DOJ of *pro forma* transaction in 2014, but not identifying the Chinese government organization that owns CITIC Group Corporation in the email correspondence or accompanying ownership charts). *But see* PN/CN April 28, 2021 Reply at 43 (stating, "[t]he Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation.").

[646] Pacific Networks, an indirect subsidiary of CITIC Group Corporation, applied for an international section 214 authorization on September 7, 2007, in which it identified the "Assets Supervision and Administration Commission of the State Council of China" (SASAC) as the Chinese government entity that "[d]irectly owns 100% of CITIC Group." Pacific Networks Corp., Application for International Section 214 Authority, File No. ITC-214-20070907-00368, Attach. 2 at 4 (filed Sept. 7, 2007). In their subsequent filings with the Commission between 2008 and 2012, Pacific Networks and ComNet continued to identify the "Assets Supervision and Administration Commission of the State Council of China" (SASAC) as the Chinese government entity that directly owns CITIC Group Corporation. *See supra* note 599.

[647] *Institution Order*, 36 FCC Rcd at 6372-73, para. 5 & n.20 (citing, for example, *CITIC Group Corporation Corporate Governance and Risk Management* ("CITIC Group . . . is a conglomerate established upon the approval of the State Council. It is funded by the Ministry of Finance on behalf of the State Council.")). According to the Ministry of Finance's website, the Ministry of Finance "implements the decisions and policies of the [Communist
(continued….)

information in the first instance, in response to the *Order to Show Cause*, especially in light of the Commission's inquiry regarding the extent of the Chinese government's ownership and control of the Companies in determining whether to revoke the Companies' section 214 authority.[648] We also find it significant that the Companies did not file *pro forma* notifications once alerted to their noncompliance. If the Ministry of Finance was always the government entity that majority-owned and controlled the Companies, the Companies provided the Commission with inaccurate information in multiple filings,[649] were required by Commission rules to correct their filings with the Commission,[650] and had ample

(Continued from previous page)
Party of China] Central Committee in the area of public finance, and adheres to the centralized and unified leadership of the [Communist Party of China] on fiscal work." Ministry of Finance of the People's Republic of China, *About Us—Main Functions*, http://www.mof.gov.cn/en/abus/mf/ (last visited Mar. 18, 2022). The "main duties" of the Ministry of Finance include, among other things, "[f]ormulating and implementing strategies, plans, policies and reform programs in the area of public finance and taxation"; "[m]anaging the central government's fiscal revenue and expenditure"; and "[c]ompiling reports on the management of state-owned assets; performing the responsibilities as the contributor to central state-owned financial capital as authorized by the State Council; formulating nationally unified regulations on the management of state-owned financial capital; formulating and implementing regulations on the management of state-owned assets in public institutions; formulating spending standards and policies that need to be nationally unified[.]" *Id.* According to SASAC's website, SASAC "is an ad hoc ministerial-level organization directly subordinated to the State Council." State-owned Assets Supervision and Administration Commission of the State Council, *About Us—What We Do*, http://en.sasac.gov.cn/2018/07/17/c_7 htm (last visited Mar. 18, 2022). SASAC, among other things, "performs the investor's responsibilities, supervises and manages the state-owned assets of enterprises under the supervision of the Central Government (excluding financial enterprises), and enhances the management of state-owned assets." *Id.* The Ministry of Finance and SASAC have different leadership within their respective organization. The leadership of the Ministry of Finance is represented by the Minister of Finance, whereas the leadership of SASAC is represented by the "Chairman" and "Party Secretary of the [Communist Party of China] Committee" of SASAC. Ministry of Finance of the People's Republic of China, *Ministers*, http://www.mof.gov.cn/en/abus/minister/ (last visited Mar. 11, 2022); *SASAC About Us*.

[648] *Institution Order*, 36 FCC Rcd at 6406-07, para. 57.

[649] *See id.* at 6372-73, para. 5 ("According to Commission records, the State-owned Assets Supervision and Administration Commission of the State Council, a Chinese government organization, directly owns 100% of CITIC Group Corporation. Other publicly available information, however, indicates that CITIC Group Corporation is funded and owned by China's Ministry of Finance."); *see also supra* notes 30, 604.

[650] For example, under section 1.65(a) of the Commission's rules, "[e]ach applicant is responsible for the continuing accuracy and completeness of information furnished in a pending application or in Commission proceedings involving a pending application. Except as otherwise required by rules applicable to particular types of applications, whenever the information furnished in the pending application is no longer substantially accurate and complete in all significant respects, the applicant shall as promptly as possible and in any event within 30 days, unless good cause is shown, amend or request the amendment of the application so as to furnish such additional or corrected information as may be appropriate. Except as otherwise required by rules applicable to particular types of applications, whenever there has been a substantial change as to any other matter which may be of decisional significance in a Commission proceeding involving the pending application, the applicant shall as promptly as possible and in any event within 30 days, unless good cause is shown, submit a statement furnishing such additional or corrected information as may be appropriate, which shall be served upon parties of record in accordance with § 1.47. . . . For the purposes of this section, an application is 'pending' before the Commission from the time it is accepted for filing by the Commission until a Commission grant or denial of the application is no longer subject to reconsideration by the Commission or to review by any court." 47 CFR § 1.65(a). Further, section 63.21(a) states that "[e]ach carrier is responsible for the continuing accuracy of the certifications made in its application [for international section 214 authority]. Whenever the substance of any such certification is no longer accurate, the carrier shall as promptly as possible and, in any event, within thirty (30) days, file with the Commission a corrected certification referencing the FCC file number under which the original certification was provided." 47 CFR § 63.21(a). As such, applicants for and holders of international section 214 authorizations are subject to the ongoing responsibility to ensure that their applications and authorizations are based on information that is factually accurate.

opportunity to do so throughout the pendency of this and prior proceedings. The Companies' conduct with respect to this information raises significant concerns about their transparency, trustworthiness, ability to cooperate with the U.S. government, and ability to comply with the Commission's rules.

124. *CITIC Tel's Role in the Companies' Management and Operations*. Based on the PSI Report, it is clear that the Companies' June 1, 2020 response to the *Order to Show Cause* omitted crucial and responsive information that ComNet previously provided to the Senate Subcommittee. Based on the record, including the Companies' subsequent April 28, 2021 filing, CITIC Tel, the Companies' indirect parent entity, has greater involvement and control over the management and operations of the Companies than was described by the Companies in their response to the *Order to Show Cause*. Specifically, the *Order to Show Cause* required the Companies to provide a detailed description of their ownership and control (direct and indirect) and "a detailed description of their corporate governance."[651] In their response to the *Order to Show Cause*, the Companies stated that "[i]n terms of day-to-day management, the Companies conduct their operations independently" and "[e]ntities upstream of [Pacific Choice International Limited] are not involved in the daily business or operations of Pacific Networks or ComNet."[652] The Companies added that "[t]he financial positions of Pacific Networks and ComNet are routinely reviewed by CITIC Tel, but they do not assess or require changes in the Companies' technical or network operations."[653]

125. Our review of the PSI Report reveals that ComNet disclosed certain information to the Senate Subcommittee that demonstrated that CITIC Tel has a much broader management role in ComNet's operations than was disclosed to the Commission in the Companies' response to the *Order to Show Cause*. The PSI Report stated that "[CITIC Tel] . . . guides ComNet on its information security policies"[654] and that while "ComNet maintains a company-specific policy . . . that policy was drafted based on [CITIC Tel's] guidance."[655] The PSI Report also revealed that ComNet actually "leverages [CITIC Tel's NOC], located in Hong Kong, for 'first tier monitoring' against cyber incidents or disruptions.'"[656] The PSI Report stated that "'[a]ll system alarms and network management data are sent to the NOC'" and "[CITIC Tel's] NOC maintains records of all alarms and access logs generated by ComNet's systems."[657] The PSI Report also indicated that "[CITIC Tel] reviews the company's budget and U.S. locations."[658] The Companies, in response to the *Order to Show Cause*, however, did not provide this information; rather, they contended that the Companies are independent, their parent entities are not involved in their operations, and CITIC Tel only "routinely" reviews their financial information.[659] Accordingly, in the *Institution Order*, we described the discrepancies between the information contained in the PSI Report and the information provided to the Commission in the Companies' response to the *Order to Show Cause*, and we stated that "ComNet's failure to provide this information to the

[651] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[652] PN/CN June 1, 2020 Response at 11; *Institution Order*, 36 FCC Rcd at 6405, para. 54.

[653] PN/CN June 1, 2020 Response at 11; *Institution Order*, 36 FCC Rcd at 6405, para. 54.

[654] PSI Report at 95-96 (citing Briefing with ComNet (Apr. 13, 2020)).

[655] *Id*. at 96.

[656] *Id*. (citing Briefing with ComNet (Apr. 13, 2020)); *see infra* para. 128. The PSI Report stated that ComNet representatives informed the Senate Subcommittee "that its daily operations are managed by its local management team in California." PSI Report at 95.

[657] PSI Report at 96 (citing to Team Telecom's records from a site visit, DHS00460PSI–65, at DHS00462PSI).

[658] *Id*. at 95 (citing Briefing with ComNet (Apr. 13, 2020)).

[659] PN/CN June 1, 2020 Response at 11.

Commission concerning the level of CITIC Tel's control suggests that the information in its filing with the Commission may be incomplete or misleading."[660]

126. With respect to the Companies' information security policy, the Companies acknowledged in their response to the *Institution Order* that they "should have clarified that while the Companies' indirect owners may not require that specific technical decisions be made on a day-to-day basis, the Companies *observe* guidance from CITIC Tel regarding network security."[661] Nonetheless, the Companies insist that they "reasonably believed information responsive to the Commission would focus on the extent to which executives of the indirect owners played a role in controlling the activities of the Companies, not on whether the Companies received any services whatsoever from affiliates."[662] The Companies argue that the *Order to Show Cause* "asked numerous very specific questions about the Companies' services, equipment and interconnection agreements" but "did not, however, similarly ask the Companies for information regarding location of databases or intercorporate arrangements, as was raised and discussed in the briefing with Senate Subcommittee staff."[663]

127. We are not persuaded by these arguments. We find that the information disclosed to the Senate Subcommittee but not to the Commission is directly relevant to the directives in the *Order to Show Cause* that the Companies provide "a description of [the Companies'] ownership and control (direct and indirect)" and "a detailed description of its corporate governance."[664] We reject the Companies' suggestion that CITIC Tel's role in the information security of the Companies' U.S. records is not relevant to the Commission's inquiry.[665] This information is critical to our assessment of the Companies' assertion that ComNet has "independence in its day-to-day operations."[666] The Companies claim that "had the Commission made clear that it considered any interaction at all between the Companies and their affiliates to be relevant (much less material) to the question of 'control' over operations . . . or asked for clarification of information in the [*Order to Show Cause*] Response as compared to information provided to the Senate Subcommittee or [sic] at any time in the almost 10 months between release of the PSI Report and release of the Order, the Companies would have provided it."[667] However, the record shows that through the CITIC Tel Information Security Policy—a policy which the Companies "observe" and that is clearly related to corporate governance—CITIC Tel exercises a level of control over the security of the Companies' U.S. records. In particular, were it not for the information contained in the PSI Report, we would not have known that the Companies observe CITIC Tel's Information Security Policy and that CITIC Tel, {[

[660] *Institution Order*, 36 FCC Rcd at 6404-08, paras. 52-59.

[661] PN/CN April 28, 2021 Reply at 69-70 (emphasis added).

[662] *Id*. at 65. While the Companies argue that, "relevant to the question of control," their response to the *Order to Show Cause* "focused on the limited nature of involvement by indirect owners and their executives," we note below that the Companies have failed *twice* to identify "all directors, officials, and other senior management" of all entities that hold 10% or greater direct or indirect interest in the Companies despite the directives in the *Order to Show Cause* and the *Institution Order*. *Id*. at 65-66; *see supra* paras. 117-20. In light of the record evidence and the Companies' repeated failure to provide complete and accurate responses to the Commission's inquiries, we find this argument proffered by the Companies to be wholly unpersuasive.

[663] PN/CN April 28, 2021 Reply at 65.

[664] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[665] The Companies argue that "the policy relates to a single aspect of ComNet's operations: handling of data security" and that "the promulgation of consistent data security policies across affiliated entities does not somehow change ComNet from having independence in its day-to-day operations to having all of its decisions dictated by indirect owners." PN/CN April 28, 2021 Reply at 68.

[666] *Id*.

[667] *See id*. at 66.

]} an integrated role in the Companies' operations and provisioning of services, including managing access to U.S. customer records by "coordinat[ing]" with the Companies.[668] The Companies attempt to characterize the CITIC Tel Information Security Policy as "consistent data security policies across affiliated entities"[669] and assert that they only "*observe* guidance from CITIC Tel regarding network security."[670] These attempts to minimize the significance of the policy, however, are undermined by the specific terms of the policy, ComNet's prior disclosures to the Senate Subcommittee, and the Companies' statement to the Commission that access to various U.S. customer records is "governed by" Section 10 of the CITIC Tel Information Security Policy.[671] Based on the preponderance of the record evidence, we therefore find that CITIC Tel has a level of control over the Companies through the CITIC Tel Information Security Policy, and that the Companies' responses regarding this issue demonstrate that the Commission cannot trust the Companies to provide accurate and complete information in their interactions with the Commission.

128. Similarly, the Companies failed to describe in their response to the *Order to Show Cause* the integrated role of CITIC Tel's Service Operations Center (SOC) {[

]} In their response to the *Institution Order*, the Companies clarify the PSI Report's statement that ComNet "leverages [CITIC's NOC],"[672] explaining that the "Network Operations Center that provides support to Pacific Networks is a different facility from the SOC that provides support to ComNet. The 'NOC' identified in the PSI Report . . . is the CITIC Tel SOC identified above and distinguished from this facility."[673] Additionally, the Companies disclose that "CITIC Tel's SOC in Hong Kong provides first tier support for ComNet's Wholesale IDD service, Retail Calling Card service, International SMS Service and VoIP services"[674] and "[o]nly the authorized monitoring system and engineer team in Hong Kong can monitor and manage the equipment in ComNet's Los Angeles data center via MPLS VPN."[675] The Companies state that {[
]} provides first tier support for Pacific Networks' MPLS VPN service"[676] and "[o]nly the authorized monitoring system and engineer team in {[ ]} can monitor and manage the equipment in Pacific Networks' facilities via a private MPLS network."[677] Further, the Companies state that {[

[668] *Id*. at 47-50; *see* PSI Report at 95-96.

[669] PN/CN April 28, 2021 Reply at 68. We reject the Companies' justification that "these policies provide the kind of protections and processes that one would expect to apply to any telecommunications or information service provider, and do so in a way that allows local management flexibility in implementation." *Id*. In this proceeding, we are specifically assessing the significant national security and law enforcement concerns associated with the Companies' ownership and control, not that of "any telecommunications or information service provider."

[670] *Id*. at 70 (emphasis added).

[671] *Id*. at 48-50.

[672] PSI Report at 96 ("ComNet leverages CITIC's network operations center ('NOC'), located in Hong Kong, for 'first tier monitoring' against cyber incidents or disruptions. 'All system alarms and network management data are sent to the NOC . . . .' Further, CITIC's NOC maintains records of all alarms and access logs generated by ComNet's systems.").

[673] PN/CN April 28, 2021 Reply at 59, n.114 (citing PSI Report at 96).

[674] *Id*. at 59.

[675] *Id*. According to the Companies, "[a]ll access to ComNet's systems through the SOC is governed by the CITIC Tel Information Security Policy." *Id.*

[676] *Id*.

[677] *Id*. According to the Companies, "[a]ll access to Pacific Networks' systems through the {[
]} is governed by the CITIC Tel Information Security Policy." *Id.*

]} "CITIC Tel's SOC in Hong Kong."[679] The Companies contend that "[t]he cybersecurity monitoring and protective service provided to ComNet by the Hong Kong SOC . . . is the same kind of service provided to telecommunications and information service providers by affiliated and third party vendors around the world."[680] They contend that "ComNet did not consider this particular fact to show 'control' by CITIC Tel or other indirect owners."[681] We are not persuaded by the Companies' claim; rather, we view this information as highly relevant to the Companies' ownership and control as it demonstrates CITIC Tel's {[ ]} involvement in and control over the Companies' technical operations.

129. Furthermore, the Companies failed to disclose to the Commission in their response to the *Order to Show Cause* highly relevant information that they provided to the Senate Subcommittee, as published in the PSI Report, concerning the extent of CITIC Tel's financial reviews and involvement in reviewing the Companies' U.S. locations. The Companies stated in response to the *Order to Show Cause* that "[t]he extent of the involvement of executives of the parent corporations of Pacific Networks and ComNet is to routinely review the financial positions of Pacific Networks and ComNet" and that "[t]hese reviews relate only to revenues from and costs of operations[.]"[682] The Companies contend that "[t]he statement that CITIC Tel 'reviews the company's budget' . . . does not contradict the statements in the [*Order to Show Cause*] Response related to involvement of ComNet's indirect owners in financial matters."[683] The Companies also argue that "[t]he statement that CITIC Tel 'reviews the company's . . . U.S. locations' does not accurately reflect CITIC Tel's limited involvement."[684] In their response to the *Institution Order*, the Companies now include information relevant to CITIC Tel's oversight of the "Companies' financial position" that should have been provided in their response to the *Order to Show*

[678] *Id.* at 53.

[679] *Id.* at 59; *id.* at 65 (referring to "CITIC Tel's Hong Kong Service Operations Center ('SOC')").

[680] *Id.* at 70. The Companies state, "it should not come as a surprise that a subsidiary of a corporation with an advanced network operations center would choose to use that facility rather than develop its own redundant facilities. None of the other numerous providers using externally provided threat monitoring would consider that outsourcing incident monitoring would in any way compromise their independent operation, and neither does ComNet: in the event of any incident ComNet's local engineers are still responsible for taking whatever actions are necessary to protect its services and customers." *Id.*

[681] *Id*. at 70-71.

[682] PN/CN June 1, 2020 Response, Declaration of LiYing (Linda) Peng. We give no merit to the Companies' argument that "[a]t most, these interactions show that CITIC Tel exerts a level of involvement with the Companies comparable to what any international corporation would exert over a small pair of subsidiaries." PN/CN *Ex Parte* Letter at 2. The relationship between the Companies and their parent entities differs from the relationship of just "any international corporation," given the fact that the Companies, through their parent entities, are ultimately majority-owned and controlled by the Chinese government, which carries significant risks, as elaborated upon above. *See supra* Sections III.B.1, III.B.2; *see supra* note 26 ("Based on the Companies' filings and our assessment, the Companies are indirectly 58.13% owned and controlled by CITIC Group Corporation and thus the Chinese government.").

[683] PN/CN April 28, 2021 Reply at 66-67 (citing PN/CN June 1, 2020 Response at 11 ("The financial positions of Pacific Networks and ComNet are routinely reviewed by CITIC Tel . . . ."); *id.* at 25 ("Non-American owners of the Companies may routinely review the financial positions of the U.S.-based Companies, in a similar fashion to how any investor might track an investment in another entity."); *id.*, Declaration of LiYing (Linda) Peng ("The extent of the involvement of executives of the parent corporations of Pacific Networks and ComNet is to routinely review the financial positions of Pacific Networks and ComNet. These reviews relate only to revenues from and costs of operations, and do not impose any specific obligations with regard to technical or commercial operations.")).

[684] *Id*. at 67.

Cause.[685] We find this omission unacceptable. We also reject the Companies' suggestion that reporting to CITIC Tel any relocation of ComNet's operations in the United States reflects "limited involvement" by the parent entity.[686] This instead shows a deeper level of control by the parent entity and should have been disclosed in response to the *Order to Show Cause*.

130. *Location of and Access to U.S. Records*. We find, as indicated in the *Institution Order*, that ComNet's interactions with the Senate Subcommittee concerning the location of U.S. records and the Companies' responses to the Commission's inquiry as to which individuals or entities have access to U.S. customer records demonstrate that the Companies cannot be trusted to provide transparent or accurate information to the Commission and Congress.[687] In the *Institution Order*, we explained that the PSI Report observed inconsistencies in the information provided to the Senate Subcommittee by ComNet and the Executive Branch agencies with regard to the location of ComNet's U.S. records.[688] The PSI Report stated, "ComNet representatives informed the Senate Subcommittee that its data center and all backed-up information are located in the United States and that it controls access to all U.S. records and data systems."[689] The PSI Report also stated that ComNet also informed the Senate Subcommittee "that its parent companies do not have direct access to these records and that they would need to request access from ComNet and follow ComNet's local procedures."[690] However, the PSI Report noted that "records of Team Telecom's site visits indicate that ComNet used [CITIC Tel's] data center in Hong Kong as a

[685] *See id*. at 43-44 (responding to directive in the *Institution Order* to provide "a detailed description of the management and oversight of Pacific Networks and ComNet by any entity that holds a [10%] or greater direct or indirect ownership interest in and/or controls Pacific Networks and ComNet" and stating, among other things, that "[o]n an annual basis, the Companies submit to CITIC Tel their Annual Operating Plan ("AOP") detailing their budgets, revenue and operating expenditures for the upcoming three years, together with the forecasted actual numbers of the current year. The AOP is prepared by each Company to show material variances between the budgeted and forecasted actual, which are then discussed with CITIC Tel. The AOP serves as the key financial performance indicator for the Companies. Monthly financial information is reported to CITIC Tel for group consolidation purposes and the Companies' local management team will explain any material variation from the AOP. As part of the oversight of the Companies' financial positions, CITIC Tel has provided guidance to the Companies from time to time regarding changes in accounting standards or specific accounting issues as they may arise."); *Institution Order*, 36 FCC Rcd at 6415, Appx. A.

[686] *See* PN/CN April 28, 2021 Reply at 67.

[687] *See Institution Order*, 36 FCC Rcd at 6406, para. 56; *id.* at 6415, Appx. A; *see infra* note 696. In the *Institution Order*, we directed the Companies to provide "a detailed response that explains the discrepancies and/or omissions, as described in this Order, concerning: (1) ComNet's statements to the Senate's Permanent Subcommittee on Investigations, as described in the PSI Report, and the statements made by Pacific Networks and ComNet in response to the Order to Show Cause; and (2) if statements made to the Commission were not accurate and complete when filed, provide accurate and complete responses to explain the discrepancies and/or omissions and to ensure the Commission has all relevant information to conduct its assessment." *Institution Order*, 36 FCC Rcd at 6416, Appx. A.

[688] *Institution Order*, 36 FCC Rcd at 6406, para. 56; PSI Report at 96.

[689] PSI Report at 96 (citing Briefing with ComNet (Apr. 13, 2020)).

[690] *Id*. (citing Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee)). *See Institution Order*, 36 FCC Rcd at 6387-88, 6406, 6410, paras. 56, 64 & nn. 132, 299. Although the PSI Report is publicly available, the underlying information upon which the Senate Subcommittee relied to reach its conclusions, such as correspondence with ComNet and any supplementary documents provided to the Senate Subcommittee by ComNet, is not in the public record. For instance, we note that the PSI Report cites to "Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee)," "Briefing with ComNet (Apr. 13, 2020)," and "ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee)." *See* PSI Report at 96-97. ComNet has not provided the Commission with copies of any written materials that it provided to the Senate Subcommittee.

backup and that ComNet's wholesale billing records 'are maintained in Hong Kong.'"[691] Further, in their response to the *Institution Order*, the Companies assert that "[d]uring ComNet's exchanges with Senate Subcommittee staff on April 13, 2020 and afterwards, ComNet representatives understood questions about the location of databases and customer records to refer only to records involved in the provision of VoIP service."[692] The Companies state that they "did not understand the Senate Subcommittee to ask about the location of databases or records related to Wholesale IDD, Retail Calling Card or MPLS VPN services."[693] Regardless of the Companies' understanding of the intent of the Senate Subcommittee, the focus of the PSI Report indicates that the Senate Subcommittee was concerned about the location of all of ComNet's records pertaining to the various communications services it provides in the United States, not only VoIP service.[694] Based on our assessment, ComNet failed to provide the Senate Subcommittee with highly relevant and material information about the location of U.S. records associated with its Wholesale IDD and Retail Calling Card services provided under its section 214 authority.[695]

131. The Companies also failed to fully respond to our directive in the *Institution Order* that they provide "an explanation and identification as to which entities and individuals have access to U.S. customer records."[696] As a result, the Companies' response provides no insight into how many individuals, including individuals associated with {[

]} With respect to ComNet's Wholesale IDD service, the Companies state that "access to records is coordinated by CITIC Tel according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy."[697] Additionally, the Companies state that {[

]}[698] The Companies, however, did not adequately identify the individuals that have access to the U.S. customer records stored in {[ ]}

132. With respect to ComNet's Retail Calling Card service, the Companies state, {[

[691] PSI Report at 96 (citing DHS00460PSI–65, at DHS00463PSI; DHS00466–71, at DHS00468PSI). The PSI Report added that "Team Telecom's records from the 2018 site visit also note that ComNet's VoIP customer and billing records are accessible to Hong Kong personnel." *Id*. (citing DHS00466–71, at DHS00470PSI).

[692] PN/CN April 28, 2021 Reply at 64. According to the Companies, "ComNet discussed the storage of VoIP service records with Senate Subcommittee staff, leading to the incorrect statement in the PSI Report that all of the Companies' service records are stored in the U.S. Originals, backups and copies of ComNet's VoIP records are only stored in the U.S., access is governed by Section 10 of the CITIC Tel Information Security Policy, and any access to such records by anyone located outside the U.S. must be authorized on an individual basis, as reported to the Senate Subcommittee Staff at the time." *Id.* at 50.

[693] *Id*. at 64.

[694] *See* PSI Report at 96.

[695] *See* PN/CN April 28, 2021 Reply at 64; *see, e.g.*, PSI Report at 95-98.

[696] *Institution Order*, 36 FCC Rcd at 6415, Appx. A. The *Institution Order* directed the Companies, "with respect to U.S. customer records, provide: (1) an identification and description of the location(s) where U.S. customer records are stored, including original records, back-up records, and copies of original records; (2) a description and copy of any policies or agreements governing access to U.S. customer records; (3) an explanation and identification as to which entities and individuals have access to U.S. customer records, how such access is granted, and any corporate policies concerning such access." *Id.*

[697] PN/CN April 28, 2021 at 48.

[698] *Id*.

]}[699] The Companies state, "[f]or this service, access to records is managed by ComNet according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy."[700] The Companies, however, did not adequately identify the individuals who have access to ComNet's U.S. customer records stored in {[ ]} Additionally, the Companies did not adequately identify the {[ ]}

133. With respect to Pacific Networks' MPLS VPN service, the Companies state that {[ ]}[701] The Companies state, "[f]or this service, access to records is coordinated by {[ ]} according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy."[702] Again, the Companies did not adequately identify these individuals who have access to the Companies' U.S. customer records stored in {[ ]} The Companies also state that "individuals employed by {[ ]} a subsidiary of CITIC Telecom have access to U.S. customer records to provide support and billing," but that "these services are provided to Pacific Networks pursuant to a services contract with {[ ]}, a subsidiary of {[ ]}"[703] However, the Companies did not mention {[ ]} in their response to the *Institution Order*'s directive to provide "an explanation and identification as to which entities and individuals have access to U.S. customer records."[704] In fact, a close reading of the services contract shows that {[ ]}[705] We find that the Companies did not provide any further information concerning {[ ]} and their failure to identify this entity as having access to U.S. records in response to the *Institution Order* is another example of the Companies' failure to provide accurate responses in this matter.

134. Importantly, the Companies state that access to ComNet's Wholesale IDD records is "coordinated" by CITIC Tel and access to Pacific Networks' MPLS VPN records is "coordinated" by {[ ]} "according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy,"[706] but the Companies did not disclose any further

[699] *Id*. at 49.

[700] *Id*.

[701] *Id*. at 49-50.

[702] *Id*.

[703] *Id*. at 72.

[704] *See id*. at 49-50.

[705] *Id*., Business Confidential Exh. J at J-3.

[706] *Id*. at 47-48, 49-50.

information on this joint coordination process, including which entity has the final decision-making authority in granting access to those records.[707] Moreover, the Companies did not explain the application of other provisions of the CITIC Tel Information Security Policy that address {[

]}[710] As we stated above, the Companies did not identify specific personnel of {[ ]} Further, the Companies did not explain whether CITIC Tel {[

[707] *Id*. at 47-50.

[708] {[ ]} *Id*., Business Confidential Exh. B at B-21. {[ ]} *See supra* paras. 117-20 (discussing the Companies' failure to fully respond to the directive to identify all officers, directors, and other senior management of all entities that hold a 10% or greater direct or indirect ownership interest in and/or control Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government.). {[ ]} *Id.*

[709] PN/CN April 28, 2021, Business Confidential Exh. B at B-22. {[ ]}

[710] *Id*.

]} Instead, the Companies vaguely assert that "[r]ecords stored outside the U.S. that are accessible by personnel outside the U.S. are only accessible to individuals that have been granted access rights in accordance with the CITIC Tel Information Security Policy, and only if necessary to provide support to the Companies."[711] Given the record, we find that the Companies failed to fully respond to the directive in the *Institution Order* and their failure to do so affirms our concerns regarding the Companies' trustworthiness and reliability.

135. *Failure to File Timely Pro Forma Notifications Concerning the 2014 Restructuring.* On May 12, 2021 and September 10, 2021, Pacific Networks and ComNet filed, respectively, notifications of the 2014 *pro forma* transfer of control, approximately seven years after the Companies were required to do so under section 63.24(f) of the Commission's rules and over a year after the Bureaus first raised the question in the *Order to Show Cause*.[712] We find that the Companies' *pro forma* notifications are deficient and therefore do not comply with our rules, further exemplifying the Companies' failure to provide the Commission with truthful and accurate information and demonstrating that they cannot be trusted to comply with our rules. In their response to the *Order to Show Cause*, the Companies admitted that "a restructuring of the CITIC Group subsidiaries in 2014 resulted in a pro forma transfer of control of Pacific Networks and ComNet for which notifications of pro forma transfer were not filed under 47 C.F.R. §63.24(f)."[713] The Companies indicated that while a corporate restructuring occurred, "[n]o material change of ultimate ownership was effected by this transaction," and after the transaction, "CITIC Group Corporation continued to control over 50% of CITIC Limited, and ultimately to control over 50% of Pacific Networks and ComNet."[714] The Companies admitted that they did not file a notification with the Commission, but did disclose the 2014 transaction to DOJ and DHS.[715] In the *Institution Order*, we stated that the Companies had yet to cure this deficiency,[716] and that "Pacific Networks' and ComNet's continued failure to file the *pro forma* notifications [after almost] seven years raises additional concerns as to whether the Commission and the U.S. government can trust Pacific Networks and ComNet to comply with U.S. law and regulations."[717]

136. We find that the Companies failed to meet the requirements of section 63.24(f) of the Commission's rules concerning notifications of *pro forma* transactions. Specifically, the Companies failed to explain with particularity the transaction that resulted in the *pro forma* transfer of control in 2014 and why such transaction was presumptively *pro forma* in nature, such as the types of transactions discussed in Note 2 to section 63.24(d) of the Commission's rules.[718] While the Companies included a

[711] *Id*. at 53.

[712] *Order to Show Cause*, 35 FCC Rcd at 3738, para. 9, n.30; *see supra* para. 8.

[713] PN/CN June 1, 2020 Response at 33.

[714] *Id*. at 6-7. The Companies state that "[t]his transfer is discussed in the [*Order to Show Cause*]." *Id*. at 6, n.19 (citing *Order to Show Cause*, 35 FCC Rcd at 3738, n.30; *id.* at 3744, Appx. B, n. 1). According to the Companies, "[t]he net result of the 2014 transfer was to replace an aggregate 100% ownership link between CITIC Group and CITIC Limited with an aggregate ownership link of 58.13%" but "the 2014 ownership change was one which did not result in a change in the actual controlling party and is therefore considered non-substantial or *pro forma*." *Id*. at 7.

[715] *Id*. at 7.

[716] *Institution Order*, 36 FCC Rcd at 6408-09, para. 60. The Companies stated that they "were alerted to the failure to file those notifications by the [*Order to Show Cause*], and are prepared to file such notifications on a *nunc pro tunc* basis or otherwise pending discussions with Commission staff on the best way to proceed." PN/CN June 1, 2020 Response at 33; *Institution Order*, 36 FCC Rcd at 6408, para. 60.

[717] *Institution Order*, 36 FCC Rcd at 6409, para. 60.

[718] *See* 47 CFR § 63.24(d), Note 2; *see* 2021 Pacific Networks Pro Forma Notification at 1 ("Further details regarding the circumstances surrounding the restructuring and the resulting transfer of control are set forth in the

(continued….)

post-transaction ownership chart, they did not explain how their ownership structure changed prior to and after the transaction.[719] Additionally, the *pro forma* notifications again do not identify the Chinese government's ownership interest, either through SASAC or the Ministry of Finance, in CITIC Group Corporation, and, therefore, the Companies.[720] While we agree with the Companies that "[n]o material change of ultimate ownership was effected by this transaction" because, following the transaction, "CITIC Group Corporation continued to control over 50% of CITIC Limited, and ultimately to control over 50% of Pacific Networks and ComNet,"[721] the Commission's rules nevertheless require all international section 214 authorization holders, including the Companies, to ensure accurate corporate ownership information is on file with the Commission and to submit any notifications of *pro forma* transfers of control within thirty (30) days of consummation pursuant to section 63.24(f).[722] At a minimum, given the significance of this proceeding, the Companies should have taken corrective action to comply with the Commission's rules immediately upon being informed of their noncompliance on April 24, 2020. We therefore view the Companies' failure to take corrective action upon being alerted to their noncompliance as demonstrating a disregard for the Commission's requirements and serving as additional evidence that the Companies cannot be relied upon to comply with the Commission's rules.[723] Given our decision to revoke and terminate the Companies' section 214 authority in this Order, we dismiss the Companies' pending *pro forma* notifications as moot.

137. Based on the overwhelming record evidence, we find that the Commission, Executive Branch agencies, and other bodies within the U.S. government cannot trust the Companies, particularly in light of the serious national security and law enforcement concerns associated with the Companies' vulnerability to exploitation, influence, and control by the Chinese government. Additionally, the Companies' omission of crucial information, failure to provide accurate and true statements to the Commission in response to the *Order to Show Cause* and *Institution Order*, and failure to comply with the Commission's rules provide evidence that the Companies cannot be trusted to comply with the Communications Act and the Commission's rules. We also find unpersuasive the Companies' attempt to justify their omissions by claiming that they had previously provided certain information to the Executive Branch agencies.[724] That the Companies may have disclosed similar information to other U.S.

(Continued from previous page)
Response to Order to Show Cause filed by Pacific Networks Corp. and ComNet (USA) LLC on June 1, 2020.") (citing PN/CN June 1, 2020 Response at 33-36); 2021 ComNet Pro Forma Notification at 1 ("Further details regarding the circumstances surrounding the restructuring and the resulting transfer of control are set forth in the Response to Order to Show Cause filed by Pacific Networks Corp. and ComNet (USA) LLC on June 1, 2020.") (citing PN/CN June 1, 2020 Response at 33-36); PN/CN June 1, 2020 Response at 33 (stating generally, "[t]he 2014 transactions restructured the arrangement of intermediate entities, and thus constituted nothing more than a pro forma transfer requiring post-consummation notification, but not requiring prior consent").

[719] *See* 2021 Pacific Networks Pro Forma Notification, Attach. at 1; 2021 ComNet Pro Forma Notification, Attach. at 1.

[720] 47 CFR § 63.24(f)(2); 47 CFR § 63.18(h); *see supra* para. 8.

[721] PN/CN June 1, 2020 Response at 6-7. The Companies state that "[t]his transfer is discussed in the [*Order to Show Cause*]." PN/CN June 1, 2020 Response at 6, n.19 (citing *Order to Show Cause*, 35 FCC Rcd at 3738, n.30; *id.* at 3744, Appx. B, n. 1).

[722] 47 CFR §§ 1.65(a), 63.21(a), 63.24(f).

[723] We find unpersuasive the Companies' attempt to justify this failure to take immediate corrective action. The Companies state, "the *Order's* comment about the Companies' 'continued failure' to file the notification is unnecessarily sharp, as the Companies stated they were prepared to file the notifications on a *nunc pro tunc* basis, but would have appreciated further discussion with Commission staff on the best way to proceed." PN/CN April 28, 2021 Reply at 16-17.

[724] PN/CN April 28, 2021 Reply at 69 (arguing, "[h]aving provided the IT policy to the U.S. government as far back as 2009, and included the then-current policy in the [*Order to Show Cause*] Response, it is not accurate to
(continued….)

government agencies does not excuse them from complying with the Commission's rules and being forthright and truthful in matters before the Commission. We expect transparency and reliability from our authorization holders as well as their compliance with the Communications Act and the Commission's rules. These qualities are simply not present here and for these reasons, which form an independent and separate basis for revocation, we revoke the Companies' section 214 authority.

C. Termination of International Section 214 Authorizations

138. Separate and apart from our findings concerning revocation of the Companies' section 214 authority, we terminate the Companies' international section 214 authorizations based on the Companies' violation of the 2009 LOA, compliance with which is an express condition of the Companies' international section 214 authorizations.[725] Pursuant to section 214(c) of the Act, the Commission "may attach to the issuance of the certificate such terms and conditions as in its judgment the public convenience and necessity may require."[726] Pacific Networks' and ComNet's international section 214 authorizations, ITC-214-20090105-00006 and ITC-214-20090424-00199, respectively, are conditioned on the Companies abiding by the commitments and undertakings contained in their 2009 LOA.[727] When the International Bureau granted an international section 214 authorization to Pacific

(Continued from previous page)
characterize the existence of the policy as a discrepancy with the PSI Report or an intentional omission of information, much less a failure of candor and transparency").

[725] April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384 ("[W]e condition grant of this application on Pacific Networks Corp. and CM Tel (USA) abiding by the commitments and undertakings set forth in their [2009 LOA] . . . ."); May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379 ("[W]e condition grant of this application on Pacific Networks Corp. and CM Tel (USA) abiding by the commitments and undertakings set forth in their [2009 LOA] . . . ."). *See Institution Order*, 35 FCC Rcd at 15033-34, para. 47 (citing *P & R Temmer v. FCC*, 743 F.2d 918 (D.C. Cir. 1984); *Atlantic Richfield Co. v. United States*, 774 F.2d 1193 (D.C. Cir. 1985); *Morris Communications, Inc. v. FCC*, 566 F.3d 184 (D.C. Cir. 2009) (automatic termination for non-payment did not violate administrative due process because in such situation "the licenses themselves . . . lapsed); *Alpine PCS, Inc. et al.; Requests for Waiver of the Installment Payment Rules and Reinstatement of Licenses*, Memorandum Opinion and Order, 25 FCC Rcd 469 (2010), *aff'd*, 404 Fed. Appx. 508 (D.C. Cir. 2010) (*Alpine PCS*) (provision for automatic cancellation did not trigger section 312(a) revocation procedures)).

[726] 47 U.S.C. § 214(c).

[727] *See* April 9, 2009 Grant Public Notice, 24 FCC Rcd at 4156; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. Under the provisions of the 2009 LOA, Pacific Networks and ComNet, among other things, agree: (1) to "make . . . U.S. Records available in the United States in response to lawful U.S. process"; (2) "to provide DHS and DOJ [within 30 days after the FCC's approval of their respective . . . license applications] an up-to-date description of: [the Companies'] physical and logical technical security architecture . . . [,] their security policies and standards . . . [,] and their information technology governance controls used to oversee CM Tel's California switching facility"; (3) "to ensure that U.S. records are not made subject to mandatory destruction under any foreign laws"; (4) "to take all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in this letter"; (5) "that they will not, directly or indirectly, disclose or permit disclosure of or access to U.S. Records, Domestic Communications . . . to any person if the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. government without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of DHS and DOJ or the authorization of a court of competent jurisdiction in the United States"; (6) "to maintain one or more points of contact within the United States with the authority and responsibility for accepting and overseeing compliance with a wiretap order, pen/trap order, subpoena or other lawful demand by U.S. law enforcement authorities for the content of communications or U.S. Records"; (7) "[w]ithin thirty (30) days of the event's occurrence, [the Companies] agree to notify DHS and DOJ:" (a) "if either commences the sale (or resale) of any services not described in this letter;" (b) "of any material changes in any of the facts as represented in [the 2009 LOA], or in notices or descriptions submitted pursuant to this letter;" (c) "of any material changes to their ownership structure" and "[m]aterial changes to ownership structure are those that would require a substantive transfer of control application or *pro forma* notification to the FCC, and those that would involve an increase or decrease
(continued….)

Networks and granted the transfer of control of ComNet's international section 214 authorization to Pacific Networks in 2009, it "condition[ed] grant of this application on [the Companies] abiding by the commitments and undertakings set forth in" the 2009 LOA to the Executive Branch agencies.[728]

139. Based on the record evidence, we find that the Companies violated the 2009 LOA by failing to "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2009 LOA]."[729] Because compliance with their commitments in the 2009 LOA is an express condition of their international section 214 authorizations, such failure warrants termination of the Companies' authorizations.[730] We recognize that the Executive Branch agencies did not formally recommend that the Commission terminate the Companies' international section 214 authorizations based on the Companies' failure to comply with the terms of the 2009 LOA, as indicated by the Companies.[731] Notwithstanding the absence of such a formal recommendation, the International Bureau expressly conditioned grant of Pacific Networks' application for international section 214 authority and grant of the Companies' application to transfer control of ComNet's international section 214 authorization to Pacific Networks on the Companies "abiding by the commitments and undertakings set forth in" the 2009 LOA. Accordingly, the Commission, under this express condition, may independently determine whether the Companies are in compliance with the 2009 LOA and their international section 214 authorizations, particularly when there is evidence of a possible violation.[732] In this case, based on our review of the record evidence and after providing the Companies with sufficient notice and opportunity to respond, we independently determine that the Companies are not in compliance with the 2009 LOA, as explained below, and we therefore terminate the underlying international section 214 authorizations.

140. *Failure to Take All Practicable Measures to Prevent Unauthorized Access to U.S. Records*. We find that the Companies failed to "take all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. Records, in violation of any U.S.

(Continued from previous page)
greater than 5% in foreign government control . . . . ;" (8) "Pacific Networks and CM Tel agree to negotiate in good faith with DHS and DOJ to resolve any national security, law enforcement and public safety concerns that DHS or DOJ may raise." 2009 LOA at 2-4.

[728] April 9, 2009 Grant Public Notice, 24 FCC Rcd at 4156; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379. The 2009 LOA provides that DHS or DOJ may request that the Commission revoke the Companies' international section 214 authorizations or take other action if the Companies breach the LOA conditions. 2009 LOA at 4 (" . . . in the event the commitments set forth in this letter are breached, in addition to any other remedy available at law or equity, DHS or DOJ may request that the FCC modify, condition, revoke, cancel, or render null and void any relevant license, permit, or other authorization granted by the FCC to Pacific Networks, CM Tel, or any successor-in-interest to either.").

[729] 2009 LOA at 2. The 2009 LOA defines "U.S. Records" as "all customer billing records, subscriber information, or any other related information used, processed, or maintained in the ordinary course of business relating to communications services offered to U.S. persons." *Id.*

[730] *See P & R Temmer v. FCC,* 743 F.2d 918; *Atlantic Richfield Co. v. United States*, 774 F.2d 1193; *see also Morris Communications, Inc. v. FCC*, 566 F.3d 184 (automatic termination for non-payment did not violate administrative due process because in such situation "the licenses themselves . . . lapsed); *Alpine PCS* (provision for automatic cancellation did not trigger section 312(a) revocation procedures).

[731] PN/CN April 28, 2021 Reply at 6 (stating, "the response not only expressly pointed out that it was not a 'recommendation,' it also stated that DoJ and Department of Homeland Security ('DHS') 'have not identified acts of non-compliance under the minimal conditions placed on the Companies' Section 214 authorizations.'") (citing Executive Branch June 4, 2021 Reply at 10).

[732] 47 U.S.C. § 214; 47 U.S.C. § 151 (The Commission's statutory obligation is "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications . . . .").

Federal, state, or local laws or of the commitments set forth in [the 2009 LOA]."[733] The Commission and the Executive Branch agencies have a strong interest in ensuring the Companies' compliance with this obligation because, as stated above, like all telecommunications carriers with access to PII, CPNI, and CDRs, the Companies have a statutory responsibility to ensure the protection of this sensitive information.[734] In particular, CPNI includes some of the most sensitive personal information that carriers and providers maintain concerning their customers as a result of their business relationship, such as phone numbers called; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.[735] Furthermore, as a condition of their international section 214 authorizations, the Companies were required to implement and take "all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. Records . . . ."[736]

141. In the *Institution Order*, we expressed concern that "[t]he record evidence warrants a closer examination of the 2009 LOA given the apparent inconsistent statements made by Pacific Networks and ComNet to the Senate Subcommittee, the Executive Branch agencies, and the Commission."[737] In this regard, we stated that the record raises questions as to "where U.S. records are actually stored and what 'practicable measures' Pacific Networks and ComNet have taken in the past and are taking presently under the specific conditions of the 2009 LOA,"[738] and such concerns "are particularly heightened in light of the national security and law enforcement concerns that the Executive Branch agencies have identified regarding Pacific Networks' and ComNet's retention of section 214 authority."[739] Accordingly, we directed the Companies to provide "a detailed description of previous and present 'practicable measures' taken to prevent unauthorized access to U.S. records as required by the 2009 LOA,"[740] and "a detailed description of what, if any, practicable measures Pacific Networks and ComNet have taken under the 2009 LOA to prevent unauthorized access if U.S. records are in fact stored

[733] 2009 LOA at 2; *see supra* note 727.

[734] *See supra* para. 82 & notes 460-63.

[735] *CPNI Order*, 22 FCC Rcd at 6931, para. 5; *see supra* note 460. The Commission's rules ensure that CPNI is adequately protected from unauthorized access, use, or disclosure. 47 CFR §§ 64.2001-.2011.

[736] 2009 LOA at 2.

[737] *Institution Order*, 36 FCC Rcd at 6410, para. 63.

[738] *Id.* at 6410-11, para. 64. In the *Institution Order*, we observed that the Companies' June 1, 2020 filing included a December 13, 2017 Letter to DOJ, in which the Companies' counsel enclosed documents, including the "CITIC Telecom IT Security Policy," "CITIC Telecom Password Control Policy Account Lockout Policy," and "CITIC Telecom User Account Policy." *Id.* at 6385, para. 27 (citing PN/CN June 1, 2020 Response, Business Confidential Exh. K at 19-22). The December 13, 2017 letter states that {[

]} PN/CN June 1, 2020 Response, Business Confidential Exh. K at 21; *Institution Order*, 36 FCC Rcd at 6385, para. 27. According to the December 13, 2017 Letter, {[

]} PN/CN June 1, 2020 Response, Business Confidential Exh. K at 21-22; *id.*, Business Confidential Exh. K at 84 ({[

]}); *Institution Order*, 36 FCC Rcd at 6385-86, para. 27. We noted that "Pacific Networks and ComNet omitted discussion of this in responding to the *Order to Show Cause*, and represented that its indirect parent entity, CITIC Tel, 'do[es] not assess or require changes in the Companies' technical or network operations.'" *Institution Order*, 36 FCC Rcd at 6385-86, para. 27 (citing PN/CN June 1, 2020 Response at 11).

[739] *Institution Order*, 36 FCC Rcd at 6410-11, para. 64.

[740] *Id.* at 6415, Appx. A.

in Hong Kong or other non-U.S. locations and accessible by their direct or indirect parent companies or other third parties."[741] As explained further below, we find that the CITIC Tel Information Security Policy, as well as the other policies described by the Companies, do not demonstrate "practicable measures" and we find that the Companies, alone, do not maintain or control access to U.S. records. Based on the record evidence, we find that the Companies therefore failed to "take all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. Records" as required by the 2009 LOA.

142. In their response to the *Institution Order*, the Companies state that "all access to U.S. records is governed by Sections 6 and 10 of the current version of the CITIC Tel Information Security Policy"[742] and that "[t]hese policies are comparable to other corporate information security policies."[743] The Companies add that they "have implemented a CPNI policy in accordance with the Commission's rules."[744] Section 6 of the CITIC Tel Information Security Policy, {[ ]}[745] Section 10 of the CITIC Tel Information Security Policy, {[ ]}[746] According to the Companies, "[a]ccess rights to the servers and {[ ]} are governed by Sections 6 and 10 of the CITIC Tel Information Security Policy . . . ."[747] The Companies state that

[741] *Id.*

[742] PN/CN April 28, 2021 Reply at 51.

[743] *Id*. The Companies state that the CITIC Tel Information Security Policy {[

]} *Id.* at 52.

[744] *Id*. at 53.

[745] *Id*., Business Confidential Exh. B at B-26-B-29; *id.,* Business Confidential Exh. B at B-26 ({[ ]}).

[746] *See id*., Business Confidential Exh. B at B-35-B-39; *id*., Business Confidential Exh. B at B-35 ({[ ]}).

[747] *Id*. at 50. *See id*. at 47-53; *id.* at 44 ("CITIC Tel has adopted policies related to information technology, security and access that have been shared with the Companies."); *id.* at 67-70. The Companies state that a {[ ]} "the Pacific Networks Corp. IT Security Policy," which ComNet had provided to the Executive Branch agencies in 2009, {[

(continued….)

"[r]ecords stored outside the U.S. that are accessible by personnel outside the U.S. are only accessible to individuals that have been granted access rights in accordance with the CITIC Tel Information Security Policy, and only if necessary to provide support to the Companies."[748]

143. In addition, the Companies state that their U.S. customer records {[ ]} and access to the records is "manage[d]" by the Companies or "coordinated" by CITIC Tel {[ ]} depending on the type of U.S. records.[749] *First*, with respect to ComNet's Retail Calling Card service, the Companies state that "access to records is managed by ComNet according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy."[750] The Companies state that {[ ]}[751] *Second*, with respect to ComNet's Wholesale IDD service, access to U.S. customer records is not protected by the Companies themselves but instead "is coordinated by CITIC Tel according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy."[752] {[ ]}[753] *Third*, with respect to Pacific Networks' MPLS VPN records, {[

(Continued from previous page)

]} *Id*. at 44, 67-68 (citing *Institution Order*, 36 FCC Rcd at 6385-86, para. 27).

[748] *Id*. at 53.

[749] *Id*. at 47-53.

[750] *Id*. at 49.

[751] *Id*. at 48-49. {[

]} *Id.*

[752] *See id*. at 48. {[

]} *Id.* at B-36.

[753] *Id*. at 47-48. Specifically, the Companies state that {[

]} *Id.*

]} "is coordinated by {[ ]} according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy."[754] The Companies state {[ ]}[755] Further, the Companies state that "individuals employed by {[ ]}, a subsidiary of [CITIC Tel], *have access to U.S. customer records to provide support and billing*."[756] The Companies further state that, among other services, "these services are provided to Pacific Networks pursuant to a services contract with {[ ]}, a subsidiary of {[ ]}[757] The types of services that {[ ]}[758]

144. Based on our review of the overall record evidence, we find that the CITIC Tel Information Security Policy is not a "practicable measure[]" that would "prevent unauthorized access to, or disclosure of the content of communications or U.S. records."[759] The Companies' representations in this matter do not assuage our concerns regarding access to and protection of U.S. records. While the Companies state that Sections 6 and 10 of the CITIC Tel Information Security Policy govern "all access to U.S. records,"[760] the Companies did not explain exactly how the Companies implement the CITIC Tel

[754] *Id*. at 50.

[755] *Id*. at 49. Specifically, the Companies state that {[ ]}

[756] PN/CN April 28, 2021 Reply at 72.

[757] *Id*.

[758] {[ ]} provides "support and billing" services and "[o]ther support services" pursuant to the services contract, {[ ]} *Id.*; *see id.,* Business Confidential Exh. J at J-1-J-12.

[759] 2009 LOA at 2.

[760] PN/CN April 28, 2021 Reply at 51.

Information Security Policy given that access to certain U.S. customer records is "coordinated" by CITIC Tel {[ ]}[761] or explain how the Companies would, among other things, enforce any security measures concerning access to {[ ]}[762] Additionally, {[ ]} and the Companies have not demonstrated how any other policy they have identified in their response shows that they are in compliance with the 2009 LOA's provision to take all practicable measures to prevent unauthorized access to and disclosure of U.S. records.[763] Furthermore, as discussed in Section III.B.3., the Companies were required to but did not identify specific personnel of {[ ]}[765] This failure to respond fully to the Commission's directive that would also assist in our analysis concerning compliance with the 2009 LOA—combined with the Companies' failure to clearly and affirmatively indicate the measures for ensuring the protection of U.S. customer records, {[ ]}—raise significant concerns and demonstrate that the Companies are not taking "all practicable measures" to protect unauthorized access to U.S. records. Based on our review of the record, we find that the Companies' arguments and representations fail to dispel serious concerns that the Companies are placing U.S. records at risk for unauthorized access and disclosure.

145. To begin, we find unacceptable the fact that the Companies are not solely responsible for protecting and governing access to ComNet's Wholesale IDD records {[ ]} and we find that the sharing of the responsibility to protect U.S. customer records does not amount to a "practicable measure[]" under the 2009 LOA. To comply with the 2009 LOA, the Companies themselves should have taken measures to ensure protection of U.S. customer records. The Companies' disclosure is significant given that the Companies did not provide any further information on this joint coordination process, including which entity has the final decision-making authority in granting access to those sensitive U.S. customer records. Based on their response, it is unclear, for example, how the Companies coordinate access to sensitive U.S. customer records, which entity keeps the record logs to

[761] *Id*. at 47-51.

[762] Notably, the Companies state that access to records associated with ComNet's Wholesale IDD service is "coordinated by CITIC Tel." *Id*. at 48. The Companies also state that access to records associated with Pacific Networks' MPLS VPN service is "coordinated by {[ ]}" *Id*. at 49-50. *See supra* note 275. The Companies do not simply "observe" CITIC Tel's Information Security Policy; rather, the Companies indicate that the CITIC Tel Information Security Policy has been a part of ComNet's information security policy since Pacific Networks acquired ComNet. PN/CN April 28, 2021 Reply at 68. *See also supra* para. 52.

[763] PN/CN April 28, 2021 Reply at 54 (discussing ComNet's CPNI policies, ComNet's privacy policy, {[ ]}).

[764] *Id*. at 72; *id.*, Business Confidential Exh. J.

[765] *See Institution Order*, 36 FCC Rcd at 6415, Appx. A. The Commission specifically asked that the Companies provide, "with respect to U.S. customer records . . . : (1) an identification and description of the location(s) where U.S. customer records are stored, including original records, back-up records, and copies of original records; (2) a description and copy of any policies or agreements governing access to U.S. customer records; (3) *an explanation and identification as to which entities and individuals have access to U.S. customer records, how such access is granted, and any corporate policies concerning such access*;" and "a description of who has access to the servers and/or data centers where U.S. customer records are located and any policies, agreements, or standards concerning access to the servers or data centers where U.S. customer records are stored." *Id.* (emphasis added).

document access, and which entity's corporate policy applies. If either CITIC Tel {[ ]} has final decision-making authority as to whether access to U.S. records is granted, we would find this to be unacceptable given that {[ ]} do not have a mitigation agreement with the Executive Branch agencies and would therefore lack the incentive to protect this sensitive information in compliance with the 2009 LOA and with U.S. law generally.

146. We also find that the CITIC Tel Information Security Policy does not amount to a "practicable measure[]" under the 2009 LOA because, rather than protecting U.S. records, it instead {[

]}[770]

147. Moreover, while the Companies emphasize the relevance of Section 10, {[

[766] PN/CN April 28, 2021 Reply, Business Confidential Exh. B at B-35 (emphasis added).

[767] *Id*.

[768] {[

]} *Id*., Business Confidential Exh. B at B-19.

[769] *See id*.

[770] Moreover, the {[

]} *Id*., Business Confidential Exh. C at C-20. The Companies identify this document, among others, as responsive to the *Institution Order*'s directive that the Companies provide "a description and copy of any policies and/or procedures in place to protect personally identifiable information (PII) and customer proprietary network information (CPNI)." *Id*. at 54 (describing {[

]}); *Institution Order*, 36 FCC Rcd at 6415, Appx. A; *see infra* note 791. {[

]} PN/CN April 28, 2021 Reply, Business Confidential Exh. C at C-20. {[

]} *See Order to Show Cause,* 35 FCC Rcd at 3737, para. 9; *Institution Order*, 36 FCC Rcd at 6415, Appx. A.

]}

148. Further, the Companies also note that in addition to Section 10, Section 6 of the CITIC Tel Information Security Policy governs "[a]ccess rights to the servers and {[ ]}[777] We find that Section 6, which covers {[ ]}[778] does not demonstrate that CITIC Tel's Information Security Policy amounts to the Companies taking "all practicable measures" to prevent unauthorized access to U.S. records. The Companies argue that the {[

[771] {[ ]} PN/CN April 28, 2021, Business Confidential Exh. B at B-14.

[772] {[ ]} *Id.*

[773] *Id*., Business Confidential Exh. B at B-22; *see supra* note 708.

[774] Further, on March 22, 2018, the Companies disclosed to the Executive Branch agencies that {[ ]} *Id*., Business Confidential Exh. D at D-28. In their response to the *Institution Order*, the Companies {[ ]} In addition to affirming our concerns regarding the Companies' lack of transparency, the Companies' representations {[ ]}

[775] *See supra* note 709; PN/CN April 28, 2021 Reply, Business Confidential Exh. B at B-22.

[776] *See supra* note 709; PN/CN April 28, 2021 Reply, Business Confidential Exh. B at B-22. {[ ]}

[777] PN/CN April 28, 2021 Reply at 50, 51-53.

[778] *See id*., Business Confidential Exh. B at B-26-B-29.

]} represent the "practicable measures" the Companies have taken to prevent unauthorized access to U.S. records in accordance with the 2009 LOA.[779] The Companies contend that these measures "are comparable to other corporate information security policies."[780] Based upon our review of the policy, Section 6 {[

]} neither of which the Companies included in their filings with the Commission.[782]

149. Most importantly, the record evidence shows that {[

]} but the Companies have not implemented practicable measures to prevent unauthorized access to these records, thereby putting U.S. records at risk for unauthorized access or disclosure. {[

]} and as discussed above, the Companies even acknowledge that {[

]}[783] Specifically, {[

]}[786] Our concern is significant {[

]}[787] *Second*, it is likely that the Companies' {[

[779] *Id*. at 51-52.

[780] *Id*. at 51.

[781] *Id*., Business Confidential Exh. B at B-26-B-27.

[782] *Id*. at B-29.

[783] *See supra* note 753.

[784] *See* PN/CN April 28, 2021 Reply at 75; *id*., Business Confidential Exh. B at B-45; *Institution Order*, 36 FCC Rcd at 6387, para. 29. {[

]} PN/CN April 28, 2021 Reply, Business Confidential Exh. B at B-45. {[

]} *Id.*

[785] PN/CN April 28, 2021 Reply at 74-75.

[786] *Id*. at 47-48, 51.

[787] In the *Institution Order*, we also noted that "other provisions of the 'CITIC Telecom IT Security Policy,' {[

]} raise national security and law enforcement concerns associated with Pacific Networks' and ComNet's ownership structure and control and the risks concerning access to their (continued….)

]} and "coordinate[]" access {[ ]} raise significant national security and law enforcement concerns.[789] {[ ]}[790] Based on our assessment, we believe that the CITIC Tel Information Security Policy does not protect the security of U.S. records or amount to "practicable measures."

150. Finally, we also find that ComNet's CPNI and Privacy Policy[791] and {[ ]} do not amount to the Companies taking "all practicable measures" to prevent unauthorized access to U.S. records.[792] Despite the Companies' contention that they have implemented a

(Continued from previous page)
networks." *Institution Order*, 36 FCC Rcd at 6387, n.128. {[ ]} PN/CN June 1, 2020 Response, Business Confidential Exh. K at 42; PN/CN April 28, 2021 Reply, Business Confidential Exh. B at B-36; *Institution Order*, 36 FCC Rcd at 6387, n.128. {[ ]} *Institution Order*, 36 FCC Rcd at 6387, n.128. {[ ]} PN/CN June 1, 2020 Response, Business Confidential Exh. K at 58; PN/CN April 28, 2021 Reply, Business Confidential Exh. B at B-53; *Institution Order*, 36 FCC Rcd at 6387, n.128. {[ ]} *Institution Order*, 36 FCC Rcd at 6387, n.128. The Companies have provided no response to these identified concerns in their response to the *Institution Order*.

[788] *See* PN/CN April 28, 2021 Reply at 49-50.

[789] *See supra* Section III.B.1 (discussing the Chinese government's influence and control over the Companies and their parent entities through, among other things, the ties of the Companies' parent entities to the Chinese Communist Party and the requirements of Chinese laws that have been enacted in recent years). The ties of the Companies' parent entities to the Chinese Communist Party, and consequently, the Chinese government, raise serious additional risks associated with {[ ]}

[790] *See* PN/CN April 28, 2021 Reply, Business Confidential Exh. J.

[791] The *Institution Order* directed the Companies to provide "a description and copy of any policies and/or procedures in place to protect personally identifiable information (PII) and customer proprietary network information (CPNI)." *Institution Order*, 36 FCC Rcd at 6415, Appx. A. In their response to the *Institution Order*, the Companies submitted copies of the following documents in response to this directive: (1) "a copy of ComNet's most recent CPNI filing," (2) "a current copy of ComNet's posted privacy policy applicable to calling card services at https://www.comnet-telecom.us/privacy-policy," {[ ]} PN/CN April 28, 2021 Reply at 54; *id.*, Business Confidential Exh. C.

[792] 2009 LOA at 2.

CPNI policy in accordance with the Commission's CPNI rules,[793] the record evidence does not show how ComNet's CPNI policy would overcome the concerns raised by the Companies' reliance on the CITIC Tel Information Security Policy with regard to preventing unauthorized access. We are also concerned with ComNet's Privacy Policy, which states that "[s]ubject to the applicable data protection laws, the Company may provide personal data to vendors and service providers who support the Company's business, such as by providing technical infrastructure services, providing customer service, facilitating payments or conducting surveys."[794] The Privacy Policy further states, "[t]he Company will use its best endeavor to ensure each of these vendors and service providers [not to] [sic] disclose or use the personal data for any other purposes."[795] The Companies, however, do not explain with specificity how ComNet uses "its best endeavor" to prevent unauthorized access or use of any personal data that it provides "to vendors and service providers who support the Company's business."[796] In fact, ComNet's Privacy Policy also states, in addressing "[t]ransfer of personal data," that "[d]epends on the nature of the services and products, the users' personal data will likely be transferred and stored in a country outside of their home country, whose data protection laws may not be the same as in the users' home country."[797] Finally, {[

]}[799] While we agree with the Companies that policies do not necessarily need to be all-encompassing {[ ]} a review of the CITIC Tel Information Security Policy and these other policies identified by the Companies, however, raises more concerns and provides no assurances that U.S. records would be protected.[800]

151. Given the record evidence, we therefore find that the Companies violated the 2009 LOA by failing to "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2009 LOA]."[801] This finding is supported by the record evidence in this case and the Executive Branch agencies' statement that "1) the [2009 LOA] is no longer adequate to protect [from] the risk posed by the Companies to law enforcement and national security interests; and 2) amending the LOA to add new mitigation measures is inadequate to protect law enforcement and national

[793] PN/CN April 28, 2021 Reply at 54.

[794] *Id*., Business Confidential Exh. C at C-14 (ComNet (USA) LLC, *Privacy Policy*, https://www.comnet-telecom.us/privacy-policy).

[795] *Id.*

[796] *Id.*

[797] *Id.* (stating, "[s]uch transfer is necessary for the performance of the services and products the users choose. Purchasing certain services and products will signify the users' explicitly consented to the proposed transfer.").

[798] *Id*., Business Confidential Exh. C at C-20.

[799] *Id*. {[ ]} *Id*.; *see supra* note 770.

[800] PN/CN April 28, 2021 Reply at 68-69 (citing *Institution Order*, 36 FCC Rcd at 6387, n.128).

[801] 2009 LOA at 2 (defining "U.S. Records" as "all customer billing records, subscriber information, or any other related information used, processed, or maintained in the ordinary course of business relating to communications services offered to U.S. persons").

security interests because the Monitoring Agencies lack confidence that the Companies will comply with additional restrictions if those obligations conflict with the [Chinese government's] updated legal requirements, which the entities in the Companies' corporate chain must follow."[802] Separate and apart from our findings concerning revocation of the Companies' section 214 authority, because the International Bureau conditioned the grant of Pacific Networks' international section 214 authorization and the grant of the transfer of control of ComNet's international section 214 authorization to Pacific Networks on the Companies "abiding by the commitments and undertakings set forth in" the 2009 LOA to the Executive Branch agencies,"[803] we terminate the Companies' international section 214 authorizations based on the Companies' violation of the 2009 LOA.

D. Mitigation Would Not Address National Security and Law Enforcement Concerns

152. Based on the record, we find that mitigation would not address the significant national security and law enforcement concerns identified in this matter. We therefore reject the Companies' suggestion that the Commission decline to revoke or terminate their section 214 authority, and instead "consider mitigation measures that will provide a trustworthy and enforceable means for the federal government to monitor the Companies' ongoing compliance."[804] We have a longstanding policy of according deference to the Executive Branch agencies' expertise in identifying and mitigating risks to national security and law enforcement interests.[805] The Executive Branch agencies state that "[a]ny mitigation agreement, no matter how complex or simple, requires a baseline level of trust between the relevant parties to the agreement, because the requisite oversight necessary to assess compliance would not necessarily be adequate to detect intentional, and possibly state-sponsored, efforts to surreptitiously violate mitigation measures."[806] The Executive Branch agencies add that a baseline "level of trust is absent here" and the agencies "lack confidence that the Companies' corporate chain will choose to meet their mitigation obligations when faced with an order from the Chinese government."[807] We agree with the Executive Branch agencies' assessment. Importantly, as discussed above, the Companies' conduct and representations to the Commission and other U.S. government agencies demonstrate that the Companies lack the trustworthiness and reliability we expect of telecommunications carriers.[808] We find that the overwhelming evidence shows that the Commission, the Executive Branch agencies, and other government agencies cannot trust or rely on the Companies to adhere to the current 2009 LOA or stricter mitigation measures, or to report any mitigation violations. The Companies' ultimate majority ownership by the Chinese government and therefore their vulnerability to exploitation, influence, and control by the Chinese government, all raise serious and substantial national security and law enforcement concerns.[809]

153. According to the Companies, further mitigation is warranted because, among other things, their "operational histories in the U.S. and record of compliance not only distinguishes them from [China Mobile USA], but also provides a far more appropriate remedy for any identified security

[802] Executive Branch June 4, 2021 Reply at 2 (citing Executive Branch Letter at 6, 10); *see infra* Section III.D.

[803] *See supra* note 725.

[804] PN/CN April 28, 2021 Reply at iii; *see* PN/CN June 1, 2020 Response at 18 (stating that "mitigation through further agreement with the Commission or Team Telecom would be entirely appropriate and warranted, given the long, positive record the Companies' have developed and their compliance efforts to date").

[805] *See supra* para. 5; *Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66.

[806] Executive Branch June 4, 2021 Reply at 3.

[807] *Id*.

[808] *See supra* Section III.B.3.

[809] *See supra* Section III.B.1.

concerns the Commission may have."[810] The Companies state that the Executive Branch did not propose additional mitigation measures and, as it clearly could have, the Executive Branch did not "request that the FCC modify, condition, revoke, cancel, or render null and void any relevant license, permit, or other authorization granted by the FCC . . . ."[811] Nevertheless, the Companies "are willing to provide additional ongoing assurances through a binding mitigation agreement to supplement or replace the existing Letter of Assurance" with additional mitigation measures.[812] With regard to the Executive Branch agencies' assessment that they cannot trust the Companies, the Companies claim that the Commission "is relying on unsupported *dicta*" to support this finding, which they state "is contradicted by the Companies' record of cooperation with Team Telecom."[813] The Companies believe, instead, that the "trust is present here."[814]

154. The Companies present no evidence or arguments that convince us that mitigation would address the serious national security and law enforcement risks identified in this Order and by the Executive Branch agencies.[815] *First*, we reject the Companies' claim that the Commission should consider further mitigation measures instead of revoking or terminating their section 214 authority because the Executive Branch agencies did not seek revocation or propose mitigation measures and because of the Companies' past cooperation with the Executive Branch agencies. As stated above, we have a longstanding policy of according deference to the Executive Branch agencies on identifying and mitigating national security and law enforcement concerns, and they have affirmatively stated in the record that they do not recommend pursuing mitigation measures here.[816]

155. *Second*, even if we were to consider mitigation measures, the Companies fail to persuasively explain how the substantial and unacceptable concerns surrounding the Companies' majority ownership by the Chinese government, access of their U.S. customer records by {[ ]} and their vulnerability to exploitation, influence, and control by the Chinese government could be mitigated entirely.[817] Although the Companies offer additional mitigation measures, such as requiring the Companies to store U.S. customer records in the United States, reporting regularly to Team Telecom, and allowing annual or semi-annual Team Telecom visits, the Companies recognize that a combination of additional measures would "not explicitly address every conceivable risk."[818] In light of the Executive Branch agencies' assessment regarding the seriousness of the national security risks arising from the Companies' operations, we do not believe the public interest would be served by pursuing mitigation measures that cannot fully address these risks.

---

[810] PN/CN June 1, 2020 Response at 31 (referencing *China Mobile USA Order*, 34 FCC Rcd at 3380, para. 38); *id*. ("The Companies have long had facilities and employees in the United States to serve their customers and, as described above . . . , they have developed a consistent record of complying with the obligations placed on them by their Letter of Assurance to Team Telecom. In almost every year since they received their Section 214 authorizations, they provided necessary updates and promptly responded with extensive materials every time they were asked. DHS and DOJ have never identified any specific security concerns.").

[811] PN/CN April 28, 2021 Reply at 18 (citing 2009 LOA at 4); PN/CN *Ex Parte* Letter at 3.

[812] PN/CN April 28, 2021 Reply at 22 (citing PN/CN June 1, 2020 Response at 25). The Companies provided a non-exhaustive list of additional mitigation measures, including: "storage of all customer records at facilities in the United States, with any redundancy also at facilities in the United States; access to customer and network records limited to United States citizens; pre-launch review of new services offered in the United States; quarterly compliance reporting under penalty of perjury; and annual or semi-annual Team Telecom site visits." *Id*.

[813] *Id*. at 20-21.

[814] PN/CN June 1, 2020 Response at iii.

[815] *See supra* Sections III.B.1, B.2, B.3.

[816] *See supra* para. 5; Executive Branch June 4, 2021 Reply at 3.

[817] *See supra* Sections III.B.1, B.2, B.3.

[818] PN/CN April 28, 2021 Reply at 22.

156. *Finally*, contrary to the Companies' arguments, the Commission is not relying on mere *dicta* regarding the Companies' trustworthiness;[819] rather, we are relying on the Executive Branch agencies' filings in the record,[820] as well as our own experience with the Companies in this matter, as discussed in detail above.[821] The Companies have shown a lack of transparency and reliability and have failed to respond fully to the Commission and Congress.[822] Based on our assessment, the Companies are not likely to cooperate and be fully transparent with the Executive Branch agencies, other agencies, and the Commission in such a way that would allow the current mitigation agreement or a more stringent mitigation agreement to be effective. We find that the national security and law enforcement risks identified here combined with the Companies' vulnerability to the exploitation, influence, and control of the Chinese government, raise substantial and serious concerns that the Companies cannot be trusted to adhere to any Executive Branch mitigation agreement in good faith and with transparency.

E. International Signaling Point Codes

157. Given the record evidence of significant national security and law enforcement risks concerning the Companies' section 214 authority, we will reclaim the two ISPCs that were provisionally assigned to ComNet in 2001 (ISPC 3-191-6) and in 2003 (ISPC 3-193-4)[823] sixty (60) days from the release date of this Order.[824] We will then make the two ISPCs available for reassignment sixty (60) days after release of the Order. Specifically, we reclaim the ISPCs because their continued use presents national security and law enforcement risks and ComNet will no longer have authority to use the ISPCs for Wholesale IDD service pursuant to the requirements in this Order. The Companies state that ComNet has been using its two ISPCs since implementation of its Wholesale IDD service.[825] The Companies state that "[w]hile the International Bureau recently reclaimed ISPCs from [China Telecom Americas and

[819] *See id*. at 21.

[820] *See* Executive Branch Nov. 16, 2020 Letter; Executive Branch June 4, 2021 Letter.

[821] *See supra* Section III.B.3.

[822] *See supra* para. 2 (finding "that the Companies' conduct and representations to the Commission and Congress demonstrate a lack of trustworthiness and reliability that erodes the baseline level of trust that the Commission and other U.S. government agencies require of telecommunications carriers given the critical nature of the provision of telecommunications service in the United States."); *see also* Section III.B.3.

[823] *See* File No. SPC-NEW-20010528-00019 (CM Tel (USA) LLC) (ISPC 3-191-6); File No. SPC-NEW-20030529-00021 (ComNet (USA) LLC) (ISPC 3-193-4) (2003 ComNet ISPC Application); International Telecommunication Union, List of International Signalling Point Codes (ISPC) (According to Recommendation ITU-T Q.708 (03/99)) (July 1, 2020), https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-Q.708B-2020-PDF-E.pdf (listing ComNet's ISPCs under the name ComNet (USA) LLC).

[824] *See* International Telecommunication Union, ITU-T Recommendation Q.708 (03/99) https://www.itu.int/rec/recommendation.asp?lang=en&parent=T-REC-Q.708-199903-I (ITU-T Recommendation Q.708); *id*. at 3 (stating that the assignment of ISPC(s) to signaling point operators is designated by each Member State's Administrator). The Commission is the Administrator of ISPCs for SS7 networks for the United States consistent with the ITU-T Recommendation Q.708. The ITU-T Recommendation Q.708 defines a signaling point code as a "code with a unique 14-bit format used at the international level for [signaling] message routing and identification of [signaling] points involved." *Id*. at 1. Such signaling points are within an SS7 switch. *Id*. For this reason, only carriers that operate their own switch would need a signaling point code. *See China Telecom Americas Institution Order*, 35 FCC Rcd at 15040, para. 58 ("ISPCs are a scarce resource that are used by international [SS7] gateways as addresses for routing domestic voice traffic to an international provider and anyone seeking an ISPC assignment is required by rule to file an application with the Commission and comply with its procedures"); *see also China Unicom Americas Order on Revocation*, FCC 22-9 at para. 121 & n.548.

[825] PN/CN June 1, 2020 Response at 16; PN/CN April 28, 2021 Reply at 76. The Companies state that they cannot now locate the letters noting the implementation date, nor do the letters appear in IBFS. PN/CN April 28, 2021 Reply at 75. The Companies further state, "the Commission [should] not, however, use the absence of such [an implementation] letter as a reason to reclaim ComNet's ISPCs." *Id.*

China Unicom Americas], in both cases the International Bureau concluded that the ISPCs were not in use,"[826] but here, "ComNet uses two ISPCs to interconnect {[ ]} through a redundant pathway, in order to provide resiliency and avoid a single point of failure."[827] We find that the record evidence does not support ComNet's retention of its two ISPCs. As discussed above, we find significant national security and law enforcement risks with the Companies retention of their section 214 authority and those same risks apply to ComNet's use of its ISPCs.[828] As required by section 9.2 of ITU-T Recommendation Q.708, ComNet must "certify conformance to the laws and regulations of the Member State in which the ISPC will be used"[829] and under section 11.6, the United States may reclaim ISPCs when the ISPCs are no longer "required by the signalling point operator."[830] This is the case here. As discussed above, ComNet must discontinue its Wholesale IDD service, and ComNet, thus, does not need the ISPCs that ComNet uses to {[

]}[831]

[826] *Id*. at 76 (citing Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, to Robert E. Stup, Jr. and Paul C. Besozzi, Counsel for China Unicom (Americas) Operations Limited, DA 21-227 (filed Mar. 10, 2021); Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, to Zhao-feng Ye and Xiaoyi Liu, China Telecom (Americas) Corporation, DA 20-1369 (filed Nov. 18, 2021). We note that the Companies refer to "China Telecom" and "China Unicom," respectively, in association with "China Telecom (Americas) Corporation" (China Telecom Americas) and "China Unicom (Americas) Operations Limited" (China Unicom Americas).

[827] PN/CN April 28, 2021 Reply at 76. The Companies state that {[

]} PN/CN June 1, 2020 Response at 16. The Companies add that {[ ]}. *Id*. The Companies add that "Wholesale IDD continues to be a major contributor to ComNet's revenue . . . ." *Id*. at 30.

[828] *See supra* Sections III.B.1, B.2, B.3.

[829] ITU-T Recommendation Q.708, Sec. 9.2 at 4.

[830] *Id*., Sec. 11.6 at 6. In its application for an ISPC in 2003, ComNet also certified that "[it is] aware that all ISPC assignments are provisional and that nobody has a property right in [an] ISPC [and it is] aware that the Commission may take an assigned ISPC and reassign it to another person." 2003 ComNet ISPC Application at 1. In that application, ComNet certified that failure to file an annual International Traffic Data Report would "be interpreted as inactive operation and could, therefore, result in the loss of the carrier's point code assignment." *Id*. In 2013, the Commission revised the International Traffic Data reporting requirements (also known as the International Traffic and Revenue reports), and eliminated them in 2017. *See Reporting Requirements for U.S. Providers of International Telecommunications Services, Amendment of Part 43 of the Commission's Rules*, IB Docket No. 04-112, Second Report and Order, 28 FCC Rcd 575 (2013); *Section 43.62 Reporting Requirements for U.S. Providers of International Services*, IB Docket Nos. 16-31, 17-55, Report and Order, 32 FCC Rcd 8115 (2017)*; 2016 Biennial Review of Telecommunications Regulations*, IB Docket Nos. 17-55, 16-131, Report and Order, 32 FCC Rcd 8115 (2017); FCC Reports, International Telecommunications Data Reports, https://go.usa.gov/xtMj4; FCC Reports, International Traffic and Revenue Reports, https://go.usa.gov/xtMpR.

[831] Our records show that ComNet (known as CM Tel (USA) LLC before 2010) failed to file an annual International Traffic Data Report with the Commission for the following years: 2001, 2002, 2003, 2005, and 2007, but support the Companies' statement that since 2009, when Pacific Networks acquired ComNet, the Companies filed annual traffic and revenue reports to reflect the two ISPCs. PN/CN April 28, 2021 Reply at 77. The Companies also state that they "are not aware of the reason why [ComNet's] prior owner did not submit Traffic and Revenue reports in 2003, 2005 and 2007." *Id*.

F. Transition Period

158. We direct the Companies to discontinue all services provided under section 214 authority no later than sixty (60) days from the release date of this Order.[832] We require the Companies to provide all affected customers with thirty (30) days' notice of service discontinuance. Such notice shall be in writing to each affected customer.[833] We further require the Companies to file a copy of the standard notice(s) sent to their customers (without providing the Commission with any customer PII information) in the docket of this proceeding through the Commission's Electronic Comment Filing System (ECFS) and the relevant file numbers in the International Bureau Filing System (IBFS) within sixty (60) days of release of this Order.[834] Additionally, as stated above, we will reclaim ComNet's two ISPCs (ISPC 3-191-6 and ISPC 3-193-4) sixty (60) days from the release date of this Order.[835]

159. We reject the Companies' request to grant them a transition period of at least twenty-four (24) months to discontinue their Retail Calling Card, Wholesale IDD, and MPLS VPN services, which are provided pursuant to section 214 authority.[836] In the *Institution Order*, we asked the Companies to provide "a complete description of all work required for [the Companies] to discontinue all section 214 services to their customers if the Commission were to revoke and/or terminate [the Companies'] section 214 authorities, along with a detailed estimate of the time required for each portion of that work and an explanation of how that estimate was reached."[837] In their response, the Companies state that "to ensure that ComNet's Calling Card customers have an opportunity to use the service they have already purchased, honor ComNet's service obligations and expiry terms and minimize disruption to ComNet's customers, ComNet would need at least 24 months to terminate Retail Calling Card service in the United States."[838] The Companies add that "it would take approximately 6-9 months to migrate third party customers and discontinue Wholesale IDD service, and as long as 24 months to migrate the seven Wholesale IDD connections provided to ComNet's [Retail] Calling Card service, given the need to maintain the connections to the {[ ]} gateway."[839] Finally, the Companies state that "[d]epending on customer need, the availability of vendors in customer areas, and the time required for finalizing the necessary arrangements and contracts acceptable to both customers and vendors/suppliers, Pacific Networks estimates that it will take approximately 12-19 months to complete migration of MPLS VPN services."[840]

---

[832] *See supra* para. 2 & note 40.

[833] *See* 47 CFR § 63.19(a)(1) ("Notice shall be in writing to each affected customer unless the Commission authorizes in advance, for good cause shown, another form of notice."); *id*. at § 63.71(a) ("Notice shall be in writing to each affected customer unless the Commission authorizes in advance, for good cause shown, another form of notice.). For ComNet's Retail Calling Card customers, the Companies may direct affected customers without a known address for receipt of written notice, through a recorded message that is played automatically when a user connects to ComNet's network access number, to written notice on ComNet's website(s) at least 30 days prior to discontinuing service. *See* PN/CN June 1, 2020 Response at 16 ("ComNet is thus not aware of the identity of customers who buy calling cards."); *see supra* para. 86. In the interest of maximizing the effectiveness of public notice, we find good cause to authorize this alternative form of notice.

[834] The Companies should follow the procedures set out in this Order rather than those in section 63.71 of the Commission's rules. 47 CFR § 63.71.

[835] *See supra* para. 157.

[836] PN/CN April 28, 2021 Reply at 77-82.

[837] *Institution Order*, 36 FCC Rcd at 6417, Appx. A.

[838] PN/CN April 28, 2021 Reply at 79.

[839] *Id*. at 80.

[840] *Id.* at 81.

160. As we described in the *China Telecom Americas Order on Revocation and Termination* and the *China Unicom Americas Order on Revocation*, the Commission's relevant discontinuance rules for international services generally provide for a thirty (30) day transition period.[841] For domestic services, the rules for discontinuance of a service by a carrier with domestic section 214 authority generally allow for discontinuance authority to be granted for non-dominant and dominant carriers, respectively, either thirty-one (31) or sixty (60) days after the application is accepted for filing.[842] The Companies have not demonstrated that their customers would be unable to obtain an adequate replacement service provider or evidence to support that their customers need a longer time period to transition to another service provider.[843]

161. *First*, with respect to the Companies' request for twenty-four (24) months to discontinue ComNet's Retail Calling Card service, the Companies indicate "that it may take as many as {[ ]} months from any given date for all unused cards issued as of that date to be used or expire."[844] The Companies, however, did not provide persuasive evidence to support this timeframe. We nevertheless could not allow ComNet to continue to honor calling card contracts for two years given the national security and law enforcement risks identified in the record. The Companies also state that, "many of ComNet's customers prefer Mandarin, Cantonese or other foreign-language customer support and would need to find an alternative provider that offers such support," but fail to provide any evidence that it would take customers such a significant time to do so.[845] *Second*, with respect to ComNet's discontinuance of the Wholesale IDD service in the United States, the Companies state that ComNet would need up to three to four months to notify customers and secure contracts, one to two months to establish new connections to the voice gateway in Hong Kong for customers wanting to continue to access the Hong Kong gateway, and an additional two weeks to complete voice quality tests on newly established circuits with all customers and launch new service.[846] Despite the Companies' claims, the burden of securing new contracts, new connections, and even test quality would normally be the responsibility of the new provider, not ComNet. *Finally*, the Companies claim that it will take approximately twelve to nineteen months to complete migration of MPLS VPN services and list a number of steps, including up to two months to send "sales representative to approach each of its customers to gauge their need for service" and allowing another 2 months to assess "the costs involved, availability of capacity, facilities or other necessary resources, or other business considerations based on customers' needs."[847] The Companies appear to be simply extending the time the Companies can provide section 214 services without providing any factual evidence to support their request. Nevertheless, the Companies'

---

[841] *China Telecom Americas Order on Revocation and Termination* at *52, para. 154. *See* 47 CFR § 63.19(a)(1).

[842] *China Telecom Americas Order on Revocation and Termination* at *52, para. 154. *See* 47 CFR § 63.71(f)(1).

[843] One factor the Commission considers in determining whether to authorize discontinuance of carrier service is the adequacy of available replacement services. *See Verizon Telephone Companies Section 63.71 Application to Discontinue Expanded Interconnection Service Through Physical Collocation*, Order, 18 FCC Rcd 22737, 22742, para. 8 (2003); *Technology Transitions et al.*, Declaratory Ruling, Second Report and Order, and Order on Reconsideration, 31 FCC Rcd 8283, 8303-04, paras. 61-62 (2016).

[844] PN/CN April 28, 2021 Reply at 78.

[845] *Id*. at 79.

[846] *Id*. at 79-80. The Companies state that "CITIC Tel would need to sign service contracts directly with the Wholesale IDD customers for access to its voice gateway in Hong Kong if they wish to continue to have such access." *Id*. at 79. The Companies add that "[s]eparate from the migration of ComNet customers, ComNet's Calling Card platform also uses the Wholesale IDD service, with a total of seven active VoIP SIP connections to the {[ ]} gateway in the Los Angeles data center." *Id.* at 80. Further, the Companies assert that "ComNet would need to continue to maintain those Wholesale IDD links for the 24 months necessary for most calling cards to expire." *Id*.

[847] *Id*. at 81.

request is not appropriate here as the national security and law enforcement concerns simply outweigh the Companies' request to grant them an extended timeframe to discontinue their provision of section 214 services.

162. As we found in the *China Telecom Americas Order on Revocation and Termination* and the *China Unicom Americas Revocation Order on Revocation*,[848] a sixty (60) day transition period providing no less than thirty (30) days' notice to customers is appropriate and should mitigate any difficulties ComNet's customers may face in finding other providers that offer Chinese-language customer support. We recognize that U.S. customers generally have many low-cost options for international calls, including to China, and at least some of these options offer Chinese-language support.[849] As we did in the past, upon release of this Order, we will seek to raise consumer awareness by issuing a consumer guide in English, Simplified Chinese, and Traditional Chinese on the Commission's website, advising ComNet's customers of our decision and raising awareness of other options for calling card services.[850]

IV. ORDERING CLAUSES

163. Accordingly, IT IS ORDERED, pursuant to sections 1, 4(i), 4(j), 214, 215, 218, and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i), 154(j), 214, 215, 218, 403, and section 1.1 of the Commission's rules, 47 CFR § 1.1, that Pacific Networks Corp.'s and ComNet (USA) LLC's domestic section 214 authority is REVOKED and their international section 214 authorizations are REVOKED AND TERMINATED.

164. IT IS FURTHER ORDERED that Pacific Networks Corp. and ComNet (USA) LLC must discontinue all services provided pursuant to section 214 authority no later than sixty (60) days from the release date of this Order.

165. IT IS FURTHER ORDERED that the *pro forma* transfer of control notifications filed by Pacific Networks Corp. and ComNet (USA) LLC ARE DISMISSED AS MOOT.

166. IT IS FURTHER ORDERED that, pursuant to sections 1, 4(i)-(j), 201-205, 211, 214, 219-220, and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i)-(j), 201-205, 211, 214, 219-220, and 403, ComNet (USA) LLC's two ISPCs (ISPC 3-191-6 and ISPC 3-193-4) will be reclaimed sixty (60) days from the release date of this Order.

167. IT IS FURTHER ORDERED that a copy of this Order on Revocation and Termination shall be sent by Certified Mail, Return Receipt Requested, and by regular first-class mail to:

Pacific Networks Corp. and ComNet (USA) LLC
c/o Jeffrey J. Carlisle
Stephen Coran
Rebecca Jacobs Goldman
David Burns
Lerman Senter PLLC

[848] *China Telecom Americas Order on Revocation and Termination* at *52, para. 152; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 130.

[849] *China Telecom Americas Order on Revocation and Termination* at *53, para. 155; *China Unicom Americas Order on Revocation*, FCC 22-9 at para. 134; *see also* Consumer Guide, FCC, Information & Resources: China Telecom (Americas) Can No Longer Provide Mobile Service in the United States; CTExcel Customers Need to Switch to a New Service Provider by January 3, 2022 (Nov. 12, 2021), https://go.usa.gov/xzBt4 (*China Telecom Americas Consumer Guide*); Consumer Guide, FCC, China Unicom to Stop U.S. Services: China Unicom Americas Can No Longer Provide Mobile Service in the United States; CUniq Customers Need to Switch to a New Service Provider by April 4, 2022 (Feb. 3, 2022), https://go.usa.gov/xzXZV (*China Unicom Americas Consumer Guide*).

[850] *China Telecom Americas Consumer Guide*; *China Unicom Americas Consumer Guide*.

2001 L Street NW, Suite 400
Washington, DC 20036

Linda Peng
General Manager, Human Resources & Administration
ComNet (USA) LLC
100 N. Barranca Street, Suite 910
West Covina, CA 91791

168. Petitions for reconsideration under section 1.106 of the Commission's rules, 47 CFR § 1.106, may be filed within thirty (30) days of the date of the release of this Order.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Pacific Networks Corp. and ComNet (USA) LLC,* GN Docket No. 20-111; ITC-214-20090105-00006; ITC-214-20090424-00199.

Communications networks depend on trust. It's fundamental. That's why during the past year the Federal Communications Commission has made it a priority to increase trust with a series of initiatives to support network security.

We kicked off the nation's first inquiry into Open RAN systems, to foster a market for more diverse and secure communications equipment. We launched a first-of-its-kind program to remove insecure equipment from domestic networks. We proposed rules to update our equipment authorization practices to better align them with national security policies and ensure that the agency does not approve insecure equipment for importation or sale in the United States. With the record in this proceeding now complete, I am pleased to announce that we will be moving forward with new rules soon. We also rechartered the Communications, Security, Reliability, and Interoperability Council with a 5G focus, and for the first time it is being co-chaired by the Cybersecurity and Infrastructure Security Agency. And just last month we launched an inquiry into Border Gateway Protocol security, to explore internet routing vulnerabilities and strengthen the cybersecurity of communications services.

At the same time, we took a close look at the foreign ownership of telecommunications companies providing service in the United States. Our efforts were informed by the recommendations and work of national security authorities. In several cases, they determined that certain state-owned enterprises could be subject to exploitation, influence, and control by foreign governments. As a result, in the last year we revoked the authorizations of China Telecom Americas and China Unicom Americas to provide communications services in the United States. Today, we continue that work and do the same for two additional companies identified by our national security colleagues—Pacific Networks Corp. and its wholly-owned subsidiary, ComNet. As before, we take this action after providing the companies with appropriate due process, including multiple opportunities to explain why we should not revoke their domestic and international authorities.

With these actions, we have a better understanding of security risks in our networks. Moreover, we have made it a priority to make these learnings public. At this time last year, we published the first-ever list of communications equipment and services that pose an unacceptable risk to national security. This is known as the Covered List. I'm pleased to report that we are again working closely with our national security partners to update this list and confirm the status of other companies that have been the subject of recent national security attention. We'll have that update later this month.

Because cyber threats are constantly evolving, so is our work. That's why earlier this year I shared with my colleagues a proposal to modernize our rules regarding data breach reporting. These rules were first adopted in 2007; it's time for an update. I look forward to the agency adopting this rulemaking without further delay because data breaches are increasing and in response we need to increase our efforts to restore network trust.

Thank you to the staff who worked on today's decision, including Stacey Ashton, Denise Coca, Kate Collins, Cole Dorsey, Francis Gutierrez, Jocelyn Jezierny, Gabrielle Kim, David Krech, Arthur Lechtman, Wayne Leighton, Adrienne McNeil, Tom Sullivan, Troy Tanner, and Patrick Webre from the International Bureau; Eduard Bartholme and Alejandro Roark from the Consumer and Governmental Affairs Bureau; Jeffrey Gee and Pam Kane from the Enforcement Bureau; Bob Cannon, Catherine Matraves, Giulia McHenry, Virginia Metallo, Donald Stockdale, Patrick Sun, and Emily Talaga from the Office of Economics and Analytics; Padma Krishnaswamy from the Office of Engineering and

Technology; Ken Carlberg, Jeffery Goldthorp, Deb Jordan, Lauren Kravetz, Nicole McGinnis, Zenji Nakazawa, Erika Olsen, and Austin Randazzo from the Public Safety and Homeland Security Bureau; Pam Arluk, Michele Berlove, Trent Harkrader, Melissa Droller Kirkel, Jodie May, Rodney McDonald, Kris Monteith, and Terri Natoli from the Wireline Competition Bureau; Monica Delong, Garnet Hanly, Susannah Larson, Jessica Quinley, and Joel Taubenblatt from the Wireless Telecommunications Bureau; and Matthew Dunne, Michele Ellison, Doug Klein, Jacob Lewis, Scott Noveck, Bill Richardson, Joel Rabinovitz, and Royce Sherlock from the Office of General Counsel.

STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *Pacific Networks Corp. and ComNet (USA) LLC*, GN Docket No. 20-111; ITC-214-20090105-00006; ITC-214-20090424-00199.

In 2019, the FCC took the then unprecedented step of blocking a wireless carrier that was owned and controlled by the Communist regime in China from connecting to our networks based on serious national security concerns. That action was entirely justified by the record and by China's evolving efforts to use entities it controls to surveil persons within our borders, steal intellectual property, and engage in other nefarious acts. Indeed, after our decision to deny China Mobile's application, I said it was time for the FCC to engage in a top-to-bottom review of every entity that would do the bidding of Communist China. As a result, we launched proceedings that focused on several entities, including China Telecom Americas, China Unicom Americas, and the two providers at issue today, Pacific Networks and ComNet.

Like those before them, we decide today to revoke the domestic and international section 214 authority of Pacific Networks and ComNet.

Our action is informed by the views submitted by the Executive Branch agencies with responsibility for national security reviews. They advised that Pacific Networks and ComNet are ultimately owned and controlled by a Chinese state-owned entity. This raises significant national security and law enforcement risks due to their susceptibility to complying with China's surveillance laws. Indeed, our own review found that the companies' continued access to U.S. telecommunications infrastructure creates opportunities for the Chinese government or other state-backed actors to engage in espionage by monitoring U.S. traffic. Our review also found that the companies' conduct towards the Commission and Congress lacked trustworthiness and reliability.

Today's action is an important one, and I am pleased that we are bringing this proceeding to a close. But there is more that the FCC and the Executive Branch must do to address the threats that Communist China continues to pose. Here are just some of those actions.

First, the FCC must ensure that our Covered List stays up to date. And we can do this in several ways. For one, we should look at adding all of the entities that have had their section 214 authorizations revoked. That would mean adding China Telecom Americas, China Unicom Americas, as well as Pacific Networks and ComNet. After all, the Executive Branch agencies' national security determinations in these proceedings appear to satisfy the statutory criteria for adding them to the Covered List, as I have noted before. For another, we should work with the Executive Branch to get their official views on other entities and whether they should be added to the Covered List—that would include Shenzhen-based drone maker DJI.

Second, we should move quickly to implement the Secure Equipment Act. The FCC sought comment last year on closing a loophole that allows entities that pose an unacceptable national security threat to continue to get their gear approved by the FCC for use in the U.S. The Secure Equipment Act gives us additional authorities to close this loophole, and we should reach a final determination in that proceeding quickly.

Third, as I and my FCC colleagues have noted, it might be possible that carriers that have their section 214 authorizations revoked based on national security concerns might be making an end run around that determination. In particular, they may be offering the same or similar services in a manner that does not require a section 214 authorization—whether that is by offering services on a private

carriage basis or providing data center or other services that do not require that type of authorization. This is not a development we can afford to ignore.

So here is one idea. I think the FCC should start a proceeding that examines whether we should prohibit regulated carriers from directly interconnecting with entities that pose a national security threat—regardless of whether those entities are providing services that require a section 214 authorization.

Fourth, as part of our top-to-bottom review, we should publish a list of every entity with an FCC license or authorization that is owned or controlled by Communist China. I would imagine that this is a fairly lengthy list. This action would help ensure that a range of stakeholders can provide any relevant information or perspectives about national security threats that these entities may pose.

In closing, I want to thank Chairwoman Rosenworcel for bringing this item up for a vote and for working diligently to secure our communications infrastructure. I also want to express my thanks to the International Bureau staff for preparing today's item for a vote. It has my support.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Pacific Networks Corp. and ComNet (USA) LLC,* GN Docket No. 20-111; ITC-214-20090105-00006; ITC-214-20090424-00199.

Our network security has never been more important. As events in Ukraine continue to unfold, reports indicate that hackers acting on behalf of Russia are seeking to sabotage Ukraine's networks – utilizing new ways of attacking critical infrastructure, financial, and governmental networks, both in cooperation with other hackers and on their own.

While we have yet to see a coordinated attack on American networks, we cannot ignore the capabilities of Russian state actors, which one technology company estimates are responsible for nearly 60 percent of all state-sponsored cyberattacks.[1] The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI recently issued a joint Cybersecurity Advisory urging organizations to take precautions against the destructive malware that has been used to target Ukrainian organizations, and CISA has updated its "Shields Up" webpage to include new cyber services and resources, recommendations, and information on how to protect critical assets. Just last week, I met with CISA's Executive Assistant Director for Cybersecurity to discuss these efforts and how our agencies can continue to work together to address threats to our nation's telecom networks.

I'm proud to say that the FCC is stepping up. I support the Chairwoman's efforts to expand our inter-agency cyber coordination and strengthen our data breach rules. I also strongly support our recent Notice of Inquiry seeking comment on security vulnerabilities of the Border Gateway Protocol (BGP), which bad actors can exploit to misroute traffic for monitoring or interception.

While Pacific Networks and ComNet don't appear to have BGP misrouting capabilities, they pose a threat similar to their fellow Chinese carriers. Like China Unicom Americas, China Telecom Americas, and China Mobile USA, Pacific Networks and ComNet are ultimately owned by a Chinese state entity, and are subject to the exploitation, influence, and control of the Chinese government. As such, they are highly likely to be forced to comply with Chinese government requests – including the accessing, monitoring, and disrupting of U.S. communications. Moreover, Pacific Networks and ComNet have failed to provide complete and accurate information to Congress and the Commission. In total, the companies' actions clearly demonstrate that they cannot be trusted to provide telecommunications service in the United States, and I support our action today.

It was almost 3 years ago that we first acted against a Chinese carrier seeking to operate in the United States. Today's decision revokes the section 214 authority for the last Chinese carriers in our country identified by Team Telecom. Taken as a whole, our actions have strengthened our national security and affirmed the FCC's statutory responsibility to protect the national defense and the safety of life and property.

Network security is national security. Today's action is another positive step towards protecting our national security, but clearly we must continue to rise to the challenges of the day. My thanks to the International Bureau and the other Bureaus and Offices that worked on this proceeding for their hard work on this item.

[1] Tom Burt, *Russian cyberattacks pose greater risk to governments and other insights from our annual report*, Microsoft On the Issues (Oct. 7, 2021), https://blogs microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/.